CRADA FINAL REPORT

Siemens-INL SCADA System Assessments:
Assessment 1: Spectrum Power TG
Assessment 2: Spectrum Power 3

Idaho National Laboratory

and

Siemens Energy, Inc.

Completed: October 9, 2013

Prepared by
Idaho National Laboratory
Idaho Falls, Idaho 83415
http://www.inl.gov
Under DOE Idaho Operations Office
Contract No. DE-AC07-05ID14517

Defer Release Until October 9, 2018

The INL is a U.S. Department of Energy National Laboratory
operated by Battelle Energy Alliance

INL/LTD-11-22614

Idaho National Laboratory

Siemens Spectrum Power TG Cyber Security Assessment Report

By
Trent Taylor
Robert Erbes
May Chaffin
Jonathan Chugg
James Thomas
Bryce Wheeler
Zackery Adams

August 2011

EXECUTIVE SUMMARY

The goal of the U.S. Department of Energy Office of Electricity Delivery and Energy Reliability (DOE/OE) National Supervisory Control and Data Acquisition (SCADA) Test Bed (NSTB) program is to enhance the reliability and resiliency of the Nation's energy infrastructure by reducing the risk of energy disruptions due to cyber attacks. A key part of the program is SCADA system vulnerability analysis that identifies and provides mitigation approaches for vulnerabilities that could put these systems at risk. A cyber security vulnerability is a weakness in a computing system that can result in harm to the system or its operation, especially when this weakness is exploited by a hostile actor or is present in conjunction with particular events or circumstances.

In 2006, DOE collaborated with energy owners and operators to develop a strategy to secure energy control systems going forward, made available through the Roadmap to Secure Control Systems in the Energy Sector. In 2011 the Roadmap was updated to keep pace with advances in technology and the evolving threat landscape, and renamed the Roadmap to Achieve Energy Delivery Systems Cyber Security. The Roadmap lays out a vision that by 2020, resilient energy delivery systems are designed, installed, operated and maintained to survive a cyber incident while sustaining critical functions. One of the Roadmap strategic directions needed to achieve this vision is to assess and monitor risk, which is the subject of this report.

A cyber security research team from Idaho National Laboratory (INL) performed a cyber security assessment of the Siemens Power Transmission and Distribution (PT&D) Spectrum Power TG system in the INL SCADA test bed from April 6 until June 30, 2011. The purpose of this assessment was to discover vulnerabilities that exist in the Power TG system and make recommendations to mitigate those vulnerabilities in the interest of protecting the critical infrastructure controlled by Power TG systems from cyber attack.

The cyber security assessment performed by INL was focused on a set of assessment targets developed in conjunction with Siemens PT&D personnel. Assessment targets reflect key components of the Power TG system an actual attacker may target to gain control of the system and cause damage to customers, employees, equipment, and competitive ability. The first part of the report provides a description of what was assessed and details of each component. The second part of the report provides the results of the INL cyber assessment along with details vulnerabilities and mitigations identified during the assessment.

During the cyber assessment, the team recognized that the Siemens PT&D Spectrum Power TG system has the following noteworthy security practices: several important vulnerabilities retested for Phase 2 were successfully resolved since being identified in Phase 1; firewall rules were improved and more consistent in Phase 2; certain Power TG services running on Windows can no longer directly give administrative privileges if compromised; several different important processes no longer allow improper administrative privileges; Phase 2 servers have fewer unnecessary services running than in Phase 1, and any remaining extraneous services have been firewalled from external access; a newer version of Microsoft Terminal Services in Phase 2 resolved a vulnerability

identified in Phase 1; the optional security package for the Power TG system was implemented well (apart from a related vulnerability, which is detailed in Section 5.3), and the security package should be standard with the system; the security posture for the Remote Terminal Unit Communication Server (RTUCS) system has improved since Phase 1 testing; and, overall, the security and quality of coding practices have improved for Phase 2.

This assessment found that the Siemens PT&D Spectrum Power TG system, as configured for this assessment, has a number of vulnerabilities associated with the planned Assessment Targets that may facilitate a successful cyber attack. The items listed below will briefly describe each vulnerability category, identify the number of occurrences, and provide a range for the score of where the vulnerability fell into the Common Vulnerability Scoring System (CVSS):

- Buffer Overflows in SCADA Services (24 instances, with CVSS scores ranging from 4.3 to 9.3)
- Web Human-Machine Interface (HMI) vulnerabilities (four instances, with CVSS scores ranging from 3.5 to 9.0)
- Improper Access Controls (Authorization) (three instances, with CVSS scores ranging from 6.4 to 9.3)
- Unpatched Published vulnerabilities (two instances, with CVSS scores of 7.3 and 8.1)
- Supervisory Control and Data Acquisition (SCADA) Data and Command Message Manipulation and Injection (two instances, with CVSS scores of 5.5 and 5.9)
- Use of Vulnerable Remote Displays Protocols (one instance, with a CVSS score of 4.7)
- Structured Query Language (SQL) Injection (one instance, with a CVSS score of 3.5).

A complete listing of all individual vulnerabilities can be found in Section 4.3.

Recommendations for mitigating the risk of the cyber attacks detailed in this report include the following:

- Mitigate buffer overflow vulnerabilities by performing input validation, a core component of secure source code development.
- Mitigate Web HMI vulnerabilities by assessing Web servers with regards to how client input is handled and filtered. Special attention should be paid to web servers that allow access to the physical system.

- Mitigate improper access controls by locking down all applications, hosts, and networks to limit the consequences of compromise as much as possible.

- Mitigate unpatched published vulnerabilities by routinely assessing all SCADA components, including operating systems, applications, services, network devices, etc., for published vulnerabilities, patching any vulnerabilities identified.

- Mitigate SCADA data and command message manipulation and injection by redesigning SCADA network protocols and the service applications that implement them for security.

- Mitigate vulnerable remote display protocols by minimizing usage, exposure, and available functionality of remote display protocols.

- Mitigate SQL injection by protecting SCADA databases. Follow the principle of least privilege. Use the strictest permissions possible on all database objects, such as execute-only for stored procedures.

Overall, the team found that while several important Phase 1 vulnerabilities were resolved before Phase 2 testing, others have yet to be mitigated, and many new vulnerabilities were found. While firewall rules were more consistent in Phase 2, the application of more detailed firewall configurations would provide additional security to the system. These issues and the vulnerabilities listed above are fully detailed in Section 5.

Finally, though the security and quality of coding practices have improved for Phase 2, the Siemens Power TG system's development spans a period of time that has seen concern over secure coding practices go from low to very high. The system's newer code generally adheres to secure coding practices while older sections of the system do not. It is strongly recommended that the older code base be refactored or rewritten in accordance with a more modern concern for secure coding practices.

CONTENTS

FIGURES

TABLES

ACRONYMS

AT	Assessment Target
CIP	Critical Infrastructure Protection
CPU	Central Processing Unit
CVE	Common Vulnerability Exposure
CVSS	Common Vulnerability Scoring System
DMZ	Demilitarized Zone
DNP	Distributed Network Protocol
DNS	Domain Name Server
DOE	U.S. Department of Energy
DOE-OE	Department of Energy Office of Electricity Delivery and Energy Reliability
DoS	Denial of Service
DQS	Dynamic Queueing System
DWH	Data Warehouse
EIP	Extended Instruction Pointer
EMS	Energy Management System
HMI	Human-Machine Interface
HP	Hewlett-Packard
HTML	Hypertext Markup Language
ICCP	Intercontrol Center Communications Protocol
ICS	Industrial Control Systems
INL	Idaho National Laboratory
IP	Internet Protocol
IPC	Interprocess Communication
LAN	Local Area Network
MitM	Man-in-the-Middle
NERC	North American Electric Reliability Corporation
NSTB	National SCADA Test Bed
PDSR	Periodic Data Storage and Retrieval
PT&D	Power Transmission and Distribution
RDBMS	Relational Database Management System
RSH	Remote Shell
RTU	Remote Terminal Unit
RTUCS	Remote Terminal Unit Communication Server

SCADA	Supervisory Control and Data Acquisition
SDB	Source Database Builder
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Socket Layer
URL	Uniform Resource Locator
VM	Virtual Machine
XDMCP	X Display Manager Control Protocol

PART 1 – ASSESSMENT PROCESS

1. INTRODUCTION

The U.S. Department of Energy (DOE) established the National Supervisory Control and Data Acquisition (SCADA) Test Bed (NSTB) to help industry and government improve the security of control systems used in the nation's energy infrastructures. The NSTB is funded and directed by the DOE Office of Electricity Delivery and Energy Reliability (DOE-OE). A key mission of the NSTB is to assess control systems for vulnerabilities that could put critical infrastructures at risk from a cyber attack.

This report describes the Idaho National Laboratory (INL) cyber security assessment of the Siemens Power Transmission and Distribution (PT&D) Spectrum Power TG Version 8.3 Service Pack 1(hereafter referred to as Power TG) system conducted in the INL Test Bed from April 6 until June 30, 2011. The Power TG system has been designed specifically for utility networks.

1.1 Assessment limitations

This report represents an attempt to assess the most critical vulnerabilities that could put the Power TG control system at risk for a cyber attack. However, it is not intended to provide a complete assessment of all the vulnerabilities associated with the Power TG control system. Furthermore, the findings and recommendations presented herein do not consider or determine compliance with National Electric Reliability Council (NERC) Critical Infrastructure Protection (CIP) Standards.

The observations and recommendations in this report are based on common security practices and the experience of the assessment team. The team does not claim to understand all of the issues affecting operation, maintenance, and architecture of the Power TG control system. Observations and recommendations made as a result of this assessment may not take into account mitigations already in place. It is also possible that operational requirements preclude implementation of some recommendations.

The assessment was performed on a baseline Power TG system configured by Siemens to represent a typical installation. No asset owner was involved in the system configuration, and the configuration does not represent any one facility. The assessment system does not include the network devices and perimeters typically found in an actual user's installation.

2. ASSESSMENT METHODOLOGY

The methodology used for the Power TG system cyber security assessment includes the following activities:

- Control system target selection

  Together with Siemens personnel, the INL assessment team identifies a list of assessment targets. These targets are specific objectives for which Siemens requested review, along with those identified to be of strategic interest to potential attackers. These targets provide the basis for subsequent assessment activities.

- Identification of vulnerabilities in selected targets

  Using a combination of commercial, proprietary, and open-source tools, the cyber assessment team discovers information about the targets that may allow the assessment team to compromise the pre-defined targets. During the course of this discovery, the assessment team may also identify additional targets.

  By documenting their course of action and the results of each activity, the assessment team characterizes the vulnerabilities as Zero Day, Published, or Configuration Induced vulnerabilities.

  Definitions:

  - **Zero Day Vulnerability.** A vulnerability discovered during the assessment that has no published corollary.

  - **Known Vulnerability.** A published vulnerability as defined by its definition in the Common Vulnerability Exposure (CVE[1]) database.

  - **Configuration-Induced Vulnerability.** A vulnerability that is created as a result of some configuration issue that may be resolved using best or recommended practices.

- Identify or develop a proof-of-concept or exploit associated with the identified vulnerabilities

  With the information gleaned from antecedent activities, the cyber assessment team attempts to exploit the vulnerabilities they have identified. If a full exploit is not cost effective, proof-of-concept code for an exploit may be developed.

- Metrics Scoring

  Using the research information, scoring metrics based on the Common Vulnerability Scoring System[2] (CVSS) are added to provide a metrics methodology for comparison with vulnerabilities from other sources based on a common methodology.

1. CVE: Common Vulnerability Exposure at http://cve.mitre.org/
2. CVSS 2.0 Guide: http://www.first.org/cvss/cvss-guide.pdf

- Recommendations for remediation of identified vulnerabilities

  Having characterized the identified vulnerabilities, the assessment team provides their best recommendation to mitigate the vulnerabilities. These recommendations are based primarily on the experience of the assessment team, and may not be feasible or reflect the operational constraints of the process control system, but should be considered as part of the reader's risk management process.

3. SYSTEM DESCRIPTION

The Spectrum Power TG Energy Management provides a real-time operating framework for the services and applications used in a SCADA system. This system that was configured for the cyber security assessment was setup to simulate the major operating components of a representative SCADA system. The basic applications and utilities provide functions that are required for the Power TG system to operate and emulate a utility system.

3.1 System Architecture

The system architecture consisted of two physical computers: a Virtual Machine (VM) Server, which was a Hewlett-Packard (HP) Server, and an HP desktop computer. The VM server was configured to run eight virtual machines, which consisted of redundant hosts (HOSTA/HOSTB), Remote Terminal Unit (RTU) Communication Server (RTUCS), workstation, web server (WEB), Source Database Builder (SDB), Data Warehouse (DWH), and an Inter-Control Center Communications Protocol (ICCP) VM. The standalone computer was configured as a workstation and an SDB client.

The system provided by Siemens for the assessment is shown below in Figure 1.

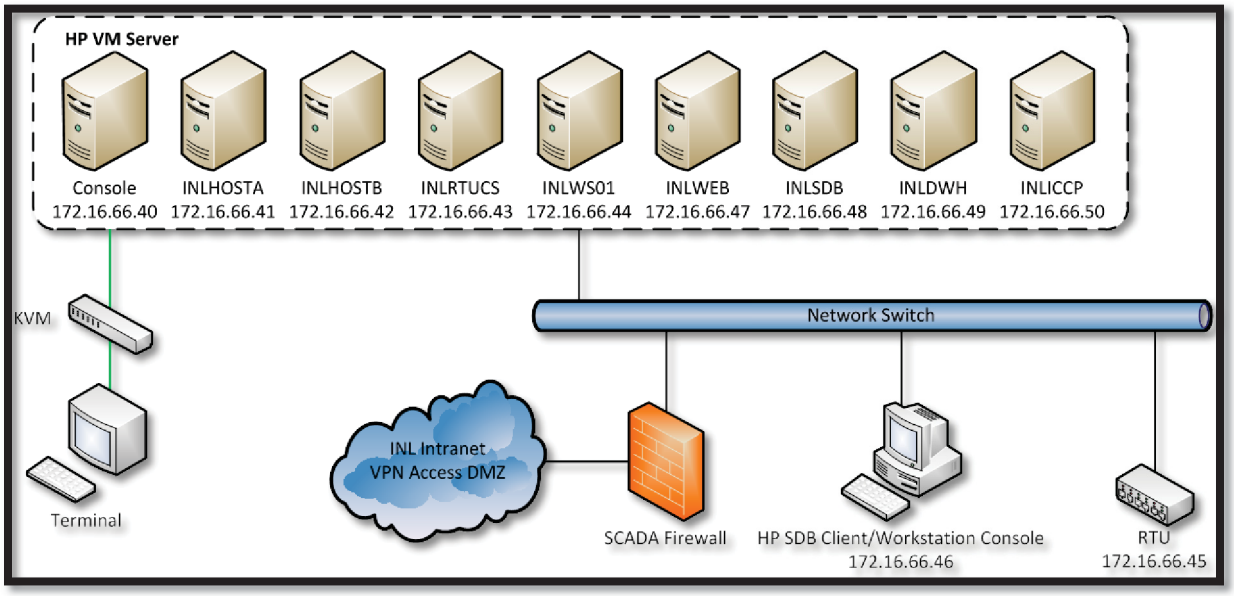


Figure 1: Power TG assessment system.

On the VM server, two SCADA/Energy Management System (EMS) hosts (INLHOSTA and INLHOSTB) were used in the assessment—both were running Red Hat Linux. Data points, communication, and console configuration were defined for the system using the SDB node (INLSDB). The SDB node on the assessment system was a VM running Windows XP. A VM running Red Hat Linux was configured as a Siemens TG workstation (INLWS01), which would connect to one of the Host servers. The Siemens TG Web Server (INLWEB) running on a Windows XP VM is used as the interface for the web services. The ICCP server (INLICCP) was a Windows XP Pro VM and also served as the Web query client for the historian. The front-end processor application for the Power TG system is called a RTUCS. The RTUCS (INLRTUCS) can be installed on any machine in the network. The Historical Server (INLDWH) is a VM that provides the capability to store operational information in a relational database, and retrieve it for analysis and other uses. The standalone desktop computer running a Windows

XP operating system served as a second workstation (INLWS02) and was also configured as an SDB Client. The final component in the system was a Station Manager RTU that was configured to handle digital and analog inputs and outputs that could be modified using the Configuration Manage Program, CMP975.

Networking for the assessment consisted of a single network with Internet Protocols (IPs) ranging from 172.16.66.40-172.

3.2 Major Components

3.2.1 INLHOSTA and INLHOSTB

3.2.1.1 Core Functions of the Hosts

Management and Database Servers provide the overall Power TG initialization and configuration management function as well as being the centralized source for the real-time database. Management and Database Servers also perform what is traditionally known as host functions. These management and coordination services include:

- System startup and initialization
- System equipment configuration control
- Data acquisition command control
- User request handler
- Real-time database management.

3.2.2 INLSDB

3.2.2.1 Core Functions of the SDB

The SDB provides a relational database environment, which is used to define and maintain most aspects of the system configuration and behavior. The SDB server supports simultaneous access by multiple users via Local Area Network (LAN) System functions provided and/or supported by the basic SDB include:

- Definition and maintenance of the Power TG equipment configuration (LANs, computers, printers, etc.)
- Definition and maintenance of the SCADA information (stations, RTUs and points) on the Power TG system
- Creation and maintenance of Power TG operator accounts
- Assignment of Areas of Responsibility
- Assignment of Areas of Viewability
- Assignment of Console Modes

- Assignment of Operator Roles
- Definition of Areas of Responsibility
- Definition of Area of Responsibility Groups
- Definition of Areas of Viewability
- Definition of point processing types
- Definition of status value translations
- Specification of processing environment options
- Alarm management and presentation
- Alarm behaviors
- Processing behaviors
- Periodic Data Storage and Retrieval (PDSR) period
- Data link (TIG/ICCP) processing parameters (requires TIG/ICCP option)
- Protocol-dependent behavior options.

3.2.3 INLRTUCS

3.2.3.1 Core Functions of the RTUCS

RTUCS handle remote and local Power TG data acquisition operations. Each RTUCS has dual-ported interfaces to redundant LANs that provide interconnections to all the client/server nodes in the system. Field data is retrieved from RTUs and other devices that are typically scanned in continuous cycles for changed information by the RTUCS. The RTUCS performs the following processing functions:

- Cyclic data acquisition from RTUs
- Management of the RTU protocols
- Engineering unit conversion of analog and accumulator values
- Analog alarm limit checking
- Monitoring and collection of communication channel statistics
- Communication channel configuration and takeover management
- Handling of local input/output devices.

3.2.4 INLWS01 and INLWS02 (Hp SDB Client/Workstation Console)

3.2.4.1 Core Functions of the workstations

User Interface Client consoles are independent workstations with their own processors, local memory, and disk storage subsystems driving single or multiple full-graphics CRTs. Each Power TG console accommodates dual connections to redundant LANs and includes interfacing support for alphanumeric keyboards, programmable function keys, audible alarms, and cursor positioning devices such as a mouse or trackball. Display formats are stored locally on each console's disk, and dynamic display descriptions are cached in console memory to achieve very fast display call-up performance. A wide range of user interface tools, such as pop-up menus and dialog boxes, provide the users with an intuitive and consistent working environment. Advanced dynamic data representations (video panel meters and real- time video trending) make it easy for the user to analyze and react to any situation quickly and accurately. Adherence to open system design principles and the use of standard communications interfaces gives Power TG User Interface Clients the capability to support remote consoles, mapboards, and video projection systems. Power TG User Interface Clients perform the following processing functions:

- Generates and updates of system displays
- Displays and manages system alarms and events
- Produces X-window full-graphic functions (panning, zooming, detail, decluttering, world coordinate processing)
- Provides online editors (interactive picture, scripting, and report editors).

3.2.5 INLWEB

3.2.5.1 Core Functions of the Web Server

The Power TG Web Console is implemented as a website providing view-only access to selected operator displays. Web Console clients must login to a valid operator account to access the website. Once the user is accepted, system displays can be requested, and zooming and panning activities performed. The clients of the Web Console site use a current or near-current release of a web browser to view the system displays. Multiple clients can be served simultaneously from a single Web Console server, and multiple Web Console servers may be incorporated into a Power TG system. Each client logged into a given Web OIS server has access to the displays available on that server. Each Web OIS server may have a different list of available displays.

3.2.6 INLDWH

3.2.6.1 Core Functions of the Data Warehouse

The Historical Server (Power TG Data Warehouse) provides the capability to store operational information in a relational database, and retrieve it for analysis, reports, playback in the SCADA/EMS environment, and other uses. Database values (analog, status, and accumulator points), alarm and event messages, and other operational data may be written and retrieved for either a subset of the database points, or all database points. The data may be written to the historian periodically, or when it changes. Archiving functions are implemented in Power TG SCADA/EMS systems with applications based on a commercially available Relational Database Management System (RDBMS). Power TG users interact

with the RDBMS using industry-standard Structured Query Language (SQL) requests. The Power TG Data Warehouse Browser product is a user-friendly tool that permits users to access historical archived data in a straightforward manner without detailed programming knowledge or experience. The interaction between the real-time database and archiving functions layered on an RDBMS include the following operations:

- Periodic/Triggered Archiving of Real-Time Data
- Archived Data Retrieval
- User Interaction with Archived Data
- Archived Data Analysis
- Archived Data Display
- Ad Hoc Report Generation
- Playback of Archive Data onto substation one-line and tabular displays.

The sets of data transferable to Archiving Servers include:

  - Telemetered information from RTUs and Field Devices
  - Calculated information from other sources
  - Other database fields from the real-time database
  - Archived Alarm and Event Messages.

3.2.7 INLICCP

3.2.7.1 Core Functions of the communications server

ICCP communication server(s) can be provided to interface with several external systems (power suppliers). The server can be provided in a non-redundant configuration or a redundant configuration with manual or automatic failover capability. The communications servers manage point-to-point datalinks and handle the complex protocol interactions required when multiple independent systems are connected together on a network. The Power TG system communications and ICCP networking applications are designed and implemented using the standard ISO/OSI interface model. The secure stack is an option that is available to prevent access to the transmitted data other than by the intended recipient.

3.3 System Operation

3.3.1 System Normal Operation Testing

Normal startup operations for the Siemens TG system was for the VM server machine to have all of the VMs started: INLHOSTA, INLHOSTB, INLRTUCS, INLWS01, INLWEB, INLSDB, INLDWH, and INLICCP. With the main VMs started the INLHOSTA Primary Server can be started and monitored during the startup process. After the startup process is complete one of the two configured workstations could be started: INLWS01 or INLWS02. From the running workstation the operator can login to the

Siemens Spectrum Power TG screen and select the System Operation screen that will provide the option to set the hot standby server online, which in this case would be the INLHOSTB machine. From this point the rest of the machines could be started and monitored from the INLWS01 screens to view their status.

Each of the above listed VMs had a snapshot taken after configuration and proper operations were tested. The snapshot for the VMs provided a quick backup and recovery process for the majority of the Siemens TG software and configuration. The standalone machine, which had the second workstation and the SDB Client, was cloned for backup and recovery needs.

With all of the backups taken and stored on a separate storage device in a secure area, the team would be able to recover any part or the entire system if needed. To perform a restore to any or all of the system the Siemens TG system would be stopped, images restored as needed, and the startup process as stated above could be used to return the system to a desired operating status.

PART 2 – ASSESSMENT RESULTS

4. ASSESSMENT OVERVIEW

The initial tasks for this assessment focused on specific Assessment Targets (AT) agreed upon by Spectrum Power TG Energy Management and the assessment team. These ATs, shown in Table 2, are based on goals of a real attacker to exploit the control system and cause damage to equipment, service, or users. The initial goals outlined are prioritized based on their potential impact to an installed Spectrum Power TG Energy Management system.

Table 2. Assessment targets.

Target No.	Target Objective	Target Description
1	Power TG Security Package	Validate the security features of the Power TG security package.
2	Gain Access to the System	Scan system computers for vulnerabilities and open ports.
3	Discover and Control the Process	Evaluate network communication between the Power TG functional packages. Attempt to perform network-based attacks to modify data.
4	RTU as a Point of Entry	Attempt to exploit the communication from an RTU to the SCADA/EMS.
5	Compromise the ICCP Server	Attempt to compromise the ICCP server from a neighboring SCADA system. Also, attempt to compromise the SCADA/EMS from the ICCP server.
6	Compromise the Historian	Attempt to compromise the Historian server by using the Historian client.

4.1 Metrics

Metrics are an important part of vulnerability assessments that provide a common methodology for evaluating vulnerabilities. With well developed and common metrics, end users have a more common basis for evaluation of risk associated with specific identified vulnerabilities.

Vulnerability research teams assessing SCADA systems and their components use the CVSS.[3] These metrics are evaluated for all vulnerabilities identified in this report.

CVSS is composed of three metric groups: Base, Temporal, and Environmental, each consisting of a set of metrics, as shown in Figure 2.

3. CVSS 2.0 Guide: http://www.first.org/cvss/cvss-guide.pdf

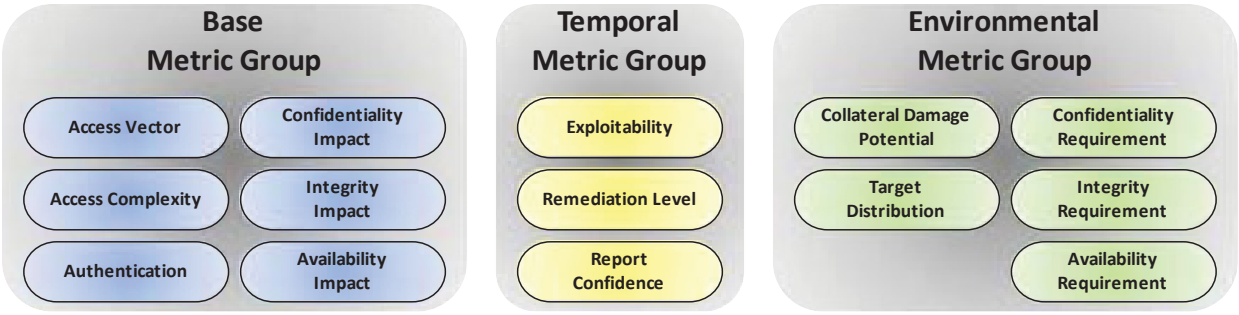


Figure 2: CVSS Metric Groups

These metric groups are described as follows:

- Base. Represents the intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments.
- Temporal. Represents the characteristics of a vulnerability that change over time but not among user environments.
- Environmental. Represents the characteristics of a vulnerability that are relevant and unique to a particular user's environment.

The purpose of the CVSS base group is to define and communicate the fundamental characteristics of a vulnerability. This objective approach to characterizing vulnerabilities provides users with a clear and intuitive representation of a vulnerability.

The purpose of the CVSS temporal group is to define the state of the vulnerability at the time this research document was published. Since it is time dependent, the metric scoring may change after publication. The end user should review this score in the context of the elapsed time since publication as the scores for this group may have changed.

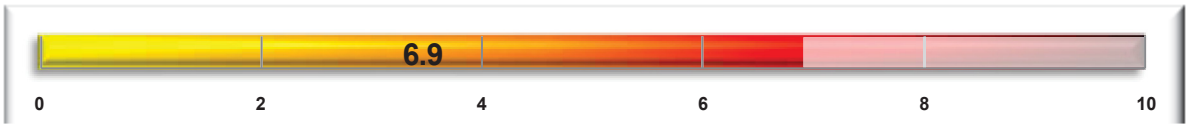
The purpose of the CVSS environmental group is to provide contextual information that more accurately reflects the risk to an end user's unique environment. This group of metrics is beyond the scope of this research document. The end user should score the environmental metric group based on their installation. This allows them to make more informed decisions on prioritization when trying to mitigate risks posed by the vulnerabilities based on the operational consequences of their installation.

4.2 Example CVSS Scoring

The CVSS scores for vulnerabilities identified in this report are generated using the National Vulnerability Database calculator[4]. An example of this scoring is shown in Table 1. The CVSS Calculator icon contains a hotlink to this web-based calculator with the values in the table automatically entered. This table is provided for each vulnerability detailed in Section 5. The web-based calculator provides the reader the option to score the Temporal and Environmental Metrics. Adding the Environmental Metrics will assist the end user in vulnerability evaluation and mitigation prioritization.

[4] NIST National Vulnerability Database; http://nvd.nist.gov/cvss.cfm?calculator&adv&version=2, link verified 8/17/11

Table 1. Sample vulnerability CVSS score.

Scoring Date:	**N/A**	
Base Score	**6.9**	 CVSS Calculator
Impact Sub score	8.5	
Exploitability Sub score	5.5	
Temporal Score	**Not Defined**	
Overall Score	**6.9**	
		
Vector	(AV:A/AC:M/Au:N/C:P/I:P/A:C/E:P/RL:W/RC:C)	

4.3 Vulnerability Summary

This section integrates the findings from the assessment into a tabular format, shown in Table 1, to identify the critical results quickly. They are sorted based on the CVSS overall score.

This sorting does not take into account the operational consequences associated with the vulnerabilities presented. To properly evaluate these consequences, the reader should evaluate the environmental metrics group for their installation and use the updated score to assist in evaluating the risks associated with the vulnerability in their installations.

A full understanding of each vulnerability listed requires that the applicable document section be carefully reviewed. Only through an understanding of the vulnerability can the reader use this information to establish the operational consequences associated with their installation.

Table 2. Summary of vulnerabilities, ratings, assessment targets, and affected components.

Vulnerability: Context	CVSS Overall Score	AT No.	Affected SCADA/EMS Components
Default User Accounts	10	1	All
Unchecked Input for Loop Condition in TGRSH Server tg_rshserver_dbcopy Function	9.3	2	Primary/backup server
ics_rbufstore_px Heap-based Buffer Overflow	9.3	3	All
api_server Process process_appl_nbr () Stack_Based Buffer Overflow	9.3	3	API/ICCP
api_server Process apisrv_process_spo_tag () Stack Based Buffer Overflow	9.3	3	API/ICCP
ProjectCA Certificate Not Validated in Certificate Chain	9.3	3	All
Scada1 SSH Server Supports Version 1	9.3	1	All
Vulnerable Versions of Open SSL Used	9.3	1	All
TG_RSH Stack-based Buffer Overflow	9.3	1	All
String Injection Allows for Code Execution	9	5	Web Server
CREATE_GROUP Large Name Stack-based Buffer Overflow	9	1	ICCP
CREATE_GROUP Large object_count DoS	7.8	1	ICCP
CREATE_GROUP Large Number of Names Dos	7.8	1	ICCP
ICS Protocol Heap-based Overflow	7.6	1	All
Data_inp Global Buffer Overflow	7.6	1	Primary/backup server
Heap_based Buffer Overflow in TGRSH Server rcpdb_expand function	7.1	2	Primary/backup server
FSP Process Invalid lanh_sendid Invalid Index/Denial of Service	7.1	3	Primary/backup server
FSP Process FILE_DESCR_U Buffer Oveflow/Denial of Service	7.1	3	Primary/backup server
Invalid Sized DQS Messages Denial of Service	7.1	1	Primary/backup server
ASUP DoS	7.1	1	Primary Server
Stack-based Buffer Overflow in TGRSH Server pcs_create_sem_pl Function	6.8	2	Primary/backup server
Stack-based Buffer Overflow in API Server API_TRACE_1 Macro	6.8	2	Primary/backup server
Stack-based Buffer Overflow in API Server apisrv_write_rts_list Function	6.8	2	Primary/backup server
Heap-Based Buffer Overflow in API Server add_connection_cli Function	6.8	2	Primary/backup server
Integer Overflow to Heap-based Buffer Overflow in RDBS Server	6.8	2	Primary/backup server
Buffer Overflow in ws_startup.exe	6.8	2	Primary/backup server
Denial of Service Through Cookie Manipulation	6.8	5	Web Server

Vulnerability: Context	CVSS Overall Score	AT No.	Affected SCADA/EMS Components
Unchecked Input for Loop Condition in API Server apisr_emsproc_nbr Function	6.8	2	Primary/backup server
Dynamic Queueing System (DQS) Message Insertion	6.6	1	Primary/backup server
Unauthorized Access to Web Server HMI	6.4	5	Web Server
tg_rshserver Common Injection	5.8	6	RTUCS
X11 and XDMCP on Power T6 Servers	5.4	1	All
Heap-based Buffer Overflow in Seriptlite Utility	4.3	2	Primary/backup server
api_server Process process_alarms_list () Denial of Service	4.3	3	API/ICCP
Data Routing Definition Form SQL Injection	3.5	4	SDB
Null Byte Injection Bypasses Display Restrictions	3.5	5	Web Server

5. ASSESSMENT TARGETS

Assessment Targets (AT) were identified in conjunction with Siemens personnel prior to the hands-on portion of the assessment, and represent steps an attacker might take to compromise the system. This section provides an overview of each AT's results. Further details for each AT are in the embedded cyber security reports included in each subsection. These embedded reports were written as stand-alone documents with the goal of recording the process such that someone similarly "skilled in the art" could reproduce the results.

5.1 Target 1 – Phase 1 Patch Verification

5.1.1 Introduction

This section attempts to extract the pertinent information from the Cyber Researcher's report on AT1. The Cyber Researcher's report documents to a level where "someone similarly skilled in the art" can reproduce the results. This level is not required for the general report. For the reader that needs this level of detail, read the attached Cyber Researcher's report: Siemens Spectrum Power TG Cyber Report for AT1 - Phase 1 Patch Verification.

5.1.2 Objective

The objective of this assessment target is to evaluate vulnerabilities identified in the Phase 1 Siemens Power TG assessment performed at INL to see if they had been patched, and if so, evaluate the efficacy of the patch.

5.1.3 Significance

Patching known vulnerabilities is vital to the process of reinforcing the security of a system.

5.1.4 Rules of Engagement

The systems delivered and set up for Phase 2 were not identical to the systems used in Phase 1. While most of these differences had little effect on the assessment, the ICCP and Historian systems were largely not testable. Time and assessment constraints, as well as technical difficulties, contributed to this issue. However, all other systems were reevaluated as described in this report.

5.1.5 Assessment

The vulnerabilities found in the Phase 1 assessment were reassessed to determine if any mitigations in the form of fixes or patches had been applied. These vulnerabilities ranged from simple configuration issues to exploited buffer overflows. Methods used in the first phase were reused to the extent possible for testing, with exceptions detailed below. Not all vulnerabilities from Phase 1 were retested, due to time constraints and technical difficulties. Table 3 provides a detailed list of these untested vulnerabilities.

Table 3. Vulnerabilities not retested for Phase 2

Vulnerability	Description
Debugging Functions Enabled on ICCP Host Web Server	The ICCP Web Server has debug methods enabled, which have known vulnerabilities, including Cross-Site Scripting (XSS).
Apache Version 2.0.50 on ICCP Host	ICCP host is running a version of Apache with a known buffer overflow exploit in mod_rewrite, plus other known issues.
PHP Version 5.0.5.5 on ICCP Host	ICCP host is running a version of PHP with known issues, including overflows.
Microsoft Windows Server Service on ICCP Host	A known overflow exists for the Microsoft Server service using the SMB protocol.
Missing localDetailCalled Field DoS	A field in the MMS initiate request message is marked as optional, but the ICCP protocol requires it. Initiate requests that omit this field cause the ICCP server to display a "Debug Assertion Failed" box, and hang until something is chosen.
Large Domain ID in Read Request Buffer Overflow	An MMS read request sent to the ICCP server with a domain specific ObjectName where the domainId field is twice the specified length causes a crash, likely a buffer overflow.
Large Item ID in Read Request Stack-based Buffer Overflow	An MMS read request sent to the ICCP server with an overly large item ID will cause a stack overflow.
ptselect.php SQL Injection Vulnerability	The $SubUID field is not validated, allowing for arbitrary SQL to be executed.
dbquery.php SQL Injection Vulnerability	The $meas variable is not filtered properly. Stripslashes is used, but can be circumvented by simply using a second backslash.
ptselect.php Persistent XSS Vulnerability	A persistent XSS vulnerability exists around the EntityName variable.
dbquery.php, savequery.php Multiple XSS Vulnerabilities	Multiple XSS vulnerabilities found in these two files.

Where vulnerabilities were still found to exist in this Phase 2 testing, a CVSS score is provided so that each vulnerability can be clearly ranked with any other vulnerabilities identified in other assessment targets. CVSS ratings are not provided for vulnerabilities that have been patched or mitigated by other means.

5.1.5.1 Configuration-induced Vulnerability: Firewalls Provide Inconsistent Filtering

The systems in both phases used firewall software included with the installed operating system. Windows servers were configured with Windows Firewall, and *iptables* was used for all Linux servers. The Phase 1 system firewall settings for each machine were inconsistent as to the filtering they provided. Several machines allowed easier access to internal services than others, providing a possible attack vector. The provided system for Phase 2 was found to have more consistent firewall rules, allowing similar access levels across all servers. While these rules do allow more consistent access between servers, they do not perform filtering based on host or subnet, which would provide additional security.

5.1.5.2 Configuration-induced Vulnerability: Default User Accounts

In the Phase 1 system, account settings for the Power TG install were found to be set to the default username “lgs” and password “1234”. These settings are listed in the Siemens Power TG documentation. Having widely documented default account settings in use allows a potential attacker to gain limited or full access easily to a service, depending on the account’s permissions. In the Phase 2 system, the account credentials were still set to defaults, leaving the vulnerability open.

5.1.5.2.1 CVSS Base Metrics

Access Vector (AV)

This vulnerability can be exploited remotely, providing the attacker can connect to the Power TG system.

The CVSS Access Vector rating is Network (N)—A vulnerability exploitable with network access means the vulnerable software is bound to the network stack, and the attacker does not require local network access or local access. Such a vulnerability is often termed “remotely exploitable.” CVSS Rating: AV:N

Access Complexity (AC)

An attacker would only need documentation or a sample system to obtain these default credentials.

The CVSS Access Complexity rating is Low (L); specialized access conditions or extenuating circumstances do not exist. CVSS Rating: AC:L

Authentication (Au)

An attacker can authenticate using these default permissions and gain control of parts of the Power TG system.

The CVSS Authentication rating is None (N); authentication is not required to access and exploit the vulnerability. CVSS Rating: Au:N

Confidentiality Impact (C)

These credentials would give an attacker privileges to obtain any available data from the Power TG system.

The CVSS Confidentiality Impact rating is Complete (C); there is a total information disclosure, resulting in all system files being revealed. Rating C:C

Integrity Impact (I)

Use of these credentials would give an attacker complete control of the system.

The CVSS Integrity Impact rating is Complete (C); there is a total compromise of system integrity. CVSS Rating: I:C

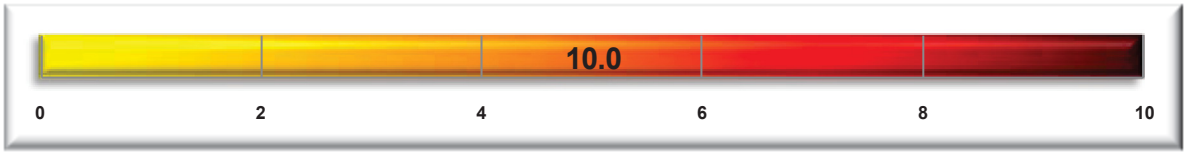
Availability Impact (A)

An attacker who gained access to the system through this account would gain the ability to shut down or damage the system.

The CVSS Availability Impact rating is Complete (C); there is a total shutdown of the affected resource. CVSS Rating: A:C

Vulnerability CVSS Score

Table 4. Default user accounts CVSS score.

Scoring Date:	**N/A**	 CVSS Calculator
Base Score	**10**	
Impact Subscore	10	
Exploitability Subscore	10	
Temporal Score	**Not Defined**	
Overall Score	**10**	
		
Vector	(AV:N/AC:L/Au:N/C:C/I:C/A:C)	

5.1.5.2.1 Mitigations

Remove default accounts, or change the password to a unique value for each installation. Additionally, administrators should ensure that strong passwords are used. The use of different passwords on each installation will help ensure that one compromised system will not easily lead to the compromise of another.

5.1.5.3 Resolved Configuration-induced Vulnerability: Windows Administrative Users

Windows servers in use for Phase 1 had accounts with administrative access running the Power TG services. These accounts can give an attacker full administrative access should a process become compromised.

As currently configured, Windows services still use the SYSTEM user account to run, but drop privileges to the “powertglocal” or “powertgremote” users before handling a client connection. These accounts lack the privileges that originally made for a privilege escalation risk.

5.1.5.3.1 Resolution

This Phase 1 vulnerability can be considered mitigated. Power TG services running on Windows hosts can no longer directly give administrative privileges if compromised.

5.1.5.4 Resolved Configuration-induced Vulnerability: tg_rshserver Privilege Escalation

The tg_rshserver process allows for remote command execution between Power TG systems. Due to these processes running under a privileged user, any commands executed by the tg_rshserver process were run with administrative rights. In the version presented for Phase 2, the process still runs as an administrative user, but drops to a less privileged user whenever a connection is established. Additionally, the security configuration for the system has been updated to define a list of allowed commands and file system accesses between specific host types (host to SDB, host to host, etc.).

5.1.5.4.1 Resolution

This specific issue can be considered resolved. The tg_rshserver process no longer executes arbitrary commands with privilege escalation as identified in the Phase 1 assessment. However, a separate vulnerability exists (see Section 5.6) that allows for similar command execution.

5.1.5.5 Configuration-induced Vulnerability: Vulnerable Versions of OpenSSL Used

Phase 1's servers used different versions of OpenSSL, depending on the host operating system installed. Linux systems used Version 0.9.7a, which has a number of known vulnerabilities.[5] The Windows systems as presented used Version 0.9.8d, which is also vulnerable to a number of attacks. The Phase 2 systems are identical in configuration with respect to OpenSSL, with the exception that the Windows servers have Version 0.9.8g installed. At the time of writing, the most current version is 1.0.0d.

5.1.5.5.1 CVSS Base Metrics

Access Vector (AV)

Encrypted communications are used when passing through the security perimeter and onto outside or less privileged networks.

The CVSS Access Vector rating is Network (N)—A vulnerability exploitable with network access means the vulnerable software is bound to the network stack, and the attacker does not require local network access or local access. Such a vulnerability is often termed "remotely exploitable." CVSS Rating: AV:N

Access Complexity (AC)

There are known exploits for the older versions of OpenSSL. However, exploits would still have to be tailored for the Power TG system in particular.

The CVSS Access Complexity rating is Medium (M); access conditions are somewhat specialized. CVSS Rating: AC:M

5. CVE vulnerabilities for OpenSSL: http://www.openssl.org/news/vulnerabilities.html

Authentication (Au)

No authentication is required to exploit this condition. Encrypted communications is used whenever the security perimeter is passed, thereby allowing an outside attacker to attack the service.

The CVSS Authentication rating is None (N); authentication is not required to access and exploit the vulnerability. CVSS Rating: Au:N

Confidentiality Impact (C)

Compromise of a buffer overflow vulnerability within OpenSSL would allow for significant or total system compromise.

The CVSS Confidentiality Impact rating is Complete (C); there is a total information disclosure, resulting in all system files being revealed. Rating C:C

Integrity Impact (I)

Compromise of a buffer overflow vulnerability within OpenSSL would allow for significant or total system compromise.

The CVSS Integrity Impact rating is Complete (C); there is a total compromise of system integrity. CVSS Rating: I:C

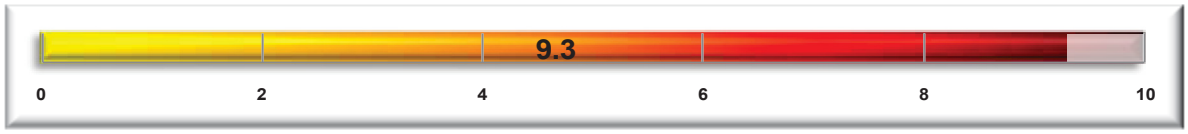
Availability Impact (A)

Compromise of the OpenSSL library would allow for complete control of the system, or a denial of service (DoS) attack.

The CVSS Availability Impact rating is Complete (C); there is a total shutdown of the affected resource. CVSS Rating: A:C

Vulnerability CVSS Score

Table 5. Vulnerable versions of OpenSSL used CVSS score.

Scoring Date:	**N/A**	 **CVSS Calculator**
Base Score	**9.3**	
Impact Subscore	10	
Exploitability Subscore	8.6	
Temporal Score	**Not Defined**	
Overall Score	**9.3**	
		
Vector	(AV:N/AC:M/Au:N/C:C/I:C/A:C)	

5.1.5.5.1 Mitigations

Up-to-date versions of OpenSSL should be distributed with Power TG systems if statically linked, and the servers themselves should be updated frequently if the library is dynamically linked.

5.1.5.5.2 Resolved Configuration-induced Vulnerability: Host Validation

In the Power TG system, the "network.asc" file defines which remote hosts may access services on a server. If the system is configured for Domain Name Server (DNS) resolution, it will perform both a forward and reverse DNS lookup on any remote host connecting to it and compare the information with this file. Otherwise, the "hosts" file is cross referenced to determine which system is attempting a connection. During Phase 1, this security feature was exploited by spoofing DNS responses. As provided, the Phase 2 system was configured with DNS disabled. This effectively eliminates the DNS spoofing vulnerability, and helps keep unauthenticated hosts from connecting to Power TG services. However, if DNS is enabled, this vulnerability still exists.

5.1.5.5.3 Resolution

Disabling DNS on the Power TG servers is an effective way to prevent an attacker from spoofing DNS requests to masquerade as an authenticated host. DNS lookups should not be used as an authenticating mechanism, as it suffers from multiple vulnerabilities including spoofing and cache poisoning.

5.1.5.6 Configuration-induced Vulnerability: Secure Socket Layer Encryption Bypass

The Power TG system allows for unencrypted communication between any two hosts that are defined as trusted. Much like the previous vulnerability, DNS spoofing allows an unauthenticated attacker to impersonate a trusted host, causing the Power TG system to forgo using encryption. In Phase 2, DNS

lookup was disabled on all servers, causing them to check their internal hosts file for lookups. However, it should be noted that enabling DNS allows this vulnerability to be exploited, and that DNS lookups alone should not be used as an authenticating mechanism.

5.1.5.6.1 Resolution

Disabling DNS lookup is a reasonably effective way to help ensure that an attacker cannot impersonate a trusted host in the current security configuration.

5.1.5.7 Resolved Configuration-induced Vulnerability: Unnecessary Services

In Phase 1, a number of services were identified as unnecessary on the Power TG system. As shipped, the servers for Phase 2 have a much smaller set of services running. Network-facing services are mainly limited to those related to Power TG. With the exception of X Display Manager Control Protocol (XDMCP), any other extraneous services are filtered at the firewall to prevent external access.

5.1.5.7.1 Resolution

Far fewer extraneous services are running on the Power TG system; those that are, have been firewalled from external access.

5.1.5.8 Configuration-induced Vulnerability: Scada1 SSH Server Supports Version 1

Both Phase 1 and Phase 2 Power TG deployments have vulnerable OpenSSH configurations installed. The installed versions support and allow fallback to the SSHv1 protocol, which has a number of known vulnerabilities. Other attacks are possible against vulnerable Secure Shell (SSH) services.

5.1.5.8.1 CVSS Base Metrics

Access Vector (AV)

A local connection is likely required to execute a MitM attack against a SSH session between hosts on a Power TG system. Other attacks may allow a more remote connection.

The CVSS Access Vector rating is Network (N)—A vulnerability exploitable with network access means the vulnerable software is bound to the network stack, and the attacker does not require local network access or local access. Such a vulnerability is often termed “remotely exploitable.” CVSS Rating: AV:N

Access Complexity (AC)

Proof of concept exploits exist for the SSHv1 protocol. The complexity depends on what method is used, as well as what network access is required.

The CVSS Access Complexity rating is Medium (M); access conditions are somewhat specialized. CVSS Rating: AC:M

Authentication (Au)

No authentication is required to execute a Man-in-the-Middle (MitM) attack or exploit other issues with the SSHv1 protocol.

The CVSS Authentication rating is None (N); authentication is not required to access and exploit the vulnerability. CVSS Rating: Au:N

Confidentiality Impact (C)

Confidentiality impact depends highly on the attack executed (MitM attack, decrypting/altering SSH traffic, etc.). However, the worst-case scenario involves complete system compromise.

The CVSS Confidentiality Impact rating is Complete (C); there is a total information disclosure, resulting in all system files being revealed. Rating C:C

Integrity Impact (I)

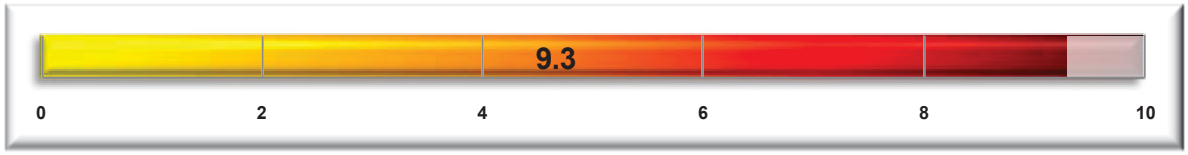
The CVSS Integrity Impact rating is Complete (C); there is a total compromise of system integrity. CVSS Rating: I:C

Availability Impact (A)

The CVSS Availability Impact rating is Complete (C); there is a total shutdown of the affected resource. CVSS Rating: A:C

Vulnerability CVSS Score

Table 6. SCADA1 SSH server supports Version 1 CVSS score.

Scoring Date:	**N/A**	 **CVSS Calculator**
Base Score	**9.3**	
Impact Subscore	10	
Exploitability Subscore	8.6	
Temporal Score	**Not Defined**	
Overall Score	**9.3**	
		
Vector	(AV:N/AC:M/Au:N/C:C/I:C/A:C)	

5.1.5.8.1 Mitigations

Upgrade to a more recent version of the OpenSSH service and libraries. Disable compatibility with Version 1 of the SSH protocol.

5.1.5.9 Configuration-induced Vulnerability: X11 and XDMCP on Power TG Servers

The XDMCP protocol is used to obtain a remote X11 graphical session on a Linux host. All Linux systems in the Power TG deployment serve the XDMCP protocol on Port 6000. In Phase 1, this port was filtered by firewall, somewhat limiting the impact of this issue. In this phase, IPv4 filtering is done, but IPv6 is ignored. XDMCP is vulnerable to MitM attacks, making it easy to obtain credentials to impersonate a legitimate user when authenticating to one of the Linux hosts.

5.1.5.9.1 CVSS Base Metrics

Access Vector (AV)

An attacker would likely need local network access to exploit a MitM condition between Power TG systems with this protocol.

The CVSS Access Vector rating is Adjacent Network (A)—A vulnerability exploitable with adjacent network ac*cess* requires the attacker to have access to either the broadcast or collision domain of the vulnerable software. CVSS Rating: AV:A

Access Complexity (AC)

Tools, such as Ettercap, are freely available that can exploit this condition.

The CVSS Access Complexity rating is Low (L); specialized access conditions or extenuating circumstances do not exist. CVSS Rating: AC:L

Authentication (Au)

An attacker does not need to authenticate to execute this attack.

The CVSS Authentication rating is None (N); authentication is not required to access and exploit the vulnerability. CVSS Rating: Au:N

Confidentiality Impact (C)

If user credentials are obtained, an attacker could gain access to the host system, but not necessarily the Power TG interfaces themselves.

The CVSS Confidentiality Impact rating is Partial (P); there is considerable informational disclosure. Rating C:P

Integrity Impact (I)

Gaining user privileges through this method would give the attacker some capability to modify the host system.

The CVSS Integrity Impact rating is Partial (P); modification of some system files or information is possible. CVSS Rating: I:P

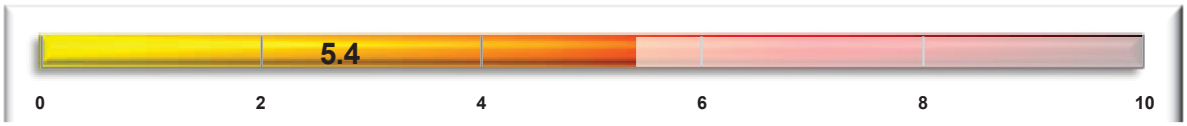
Availability Impact (A)

An attacker could gain user privileges using this method, but would still need to tailor an attack on the SCADA system itself.

The CVSS Availability Impact rating is Partial (P); there is reduced performance or interruptions in resource availability. CVSS Rating: A:P

Vulnerability CVSS Score

Table 7. X11 and XDMCP on SCADA1 CVSS score.

Scoring Date:	**N/A**	 **CVSS Calculator**
Base Score	**5.4**	
Impact Subscore	6.4	
Exploitability Subscore	5.5	
Temporal Score	**Not Defined**	
Overall Score	**5.4**	
		
Vector	(AV:A/AC:M/Au:N/C:P/I:P/A:P)	

5.1.5.9.1 Mitigations

Restrict access to Port 6000, or if XDMCP is not used, disable the functionality entirely.

5.1.5.10 Resolved Configuration-induced Vulnerability: Microsoft Terminal Server Man-in-the-Middle

Older versions of the Microsoft Terminal Services suffer from a vulnerability[6] that can lead to a MitM attack. The Phase 1 deployment's Windows servers came with an affected version, while the Phase 2 servers used a newer version of Windows Server and Terminal Services. This newer version is not known to be vulnerable to the same attack.

5.1.5.10.1 Resolution

Using a newer version of Microsoft Terminal Services resolved this issue.

5.1.5.11 Zero-Day Vulnerability: Dynamic Queueing System (DQS) Message Insertion

The DQS is a shared queue that the Power TG system uses to pass data from one process to another. Unlike most Interprocess Communication (IPC) systems, this one is network accessible. Four processes are known to forward messages to the DQS queue, and the *wslan_server* process was tested specifically. This vulnerability was exploited by reverse engineering the network protocol used and

6. Terminal Services CVE: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-1794

attempting to send forged messages through the *wslan_server* process. Proof of concept code was written to shut down the EMS system, and to insert and delete alarms from the system.

This vulnerability was retested using the proof of concept code from the first phase, and the service was still found to be vulnerable to arbitrary command injection.

5.1.5.11.1 CVSS Base Metrics

Access Vector (AV)

The DQS queue is remotely accessible, and some services that support injecting messages into the queue run on less privileged machines (e.g., workstations).

The CVSS Access Vector rating is Network (N)—A vulnerability exploitable with network access means the vulnerable software is bound to the network stack, and the attacker does not require local network access or local access. Such a vulnerability is often termed "remotely exploitable." CVSS Rating: AV:N

Access Complexity (AC)

Determining vulnerable services and designing malicious DQS messages requires a significant amount of effort.

The CVSS Access Complexity rating is High (H); specialized access conditions exist. CVSS Rating: AC:H

Authentication (Au)

The DQS queue has no authentication mechanism; an attacker can inject messages anonymously.

The CVSS Authentication rating is None (N); authentication is not required to access and exploit the vulnerability. CVSS Rating: Au:N

Confidentiality Impact (C)

Controlling the DQS queue gives an attacker control of several processes.

The CVSS Confidentiality Impact rating is Partial (P); there is considerable informational disclosure. Rating C:P

Integrity Impact (I)

Control of the DQS queue mainly confers the ability to control or modify running processes. Few processes run with administrative privileges at this time, and root access is unlikely.

The CVSS Integrity Impact rating is Partial (P); modification of some system files or information is possible. CVSS Rating: I:P

Availability Impact (A)

DQS messages include the ability to completely shut down the EMS.

The CVSS Availability Impact rating is Complete (C); there is a total shutdown of the affected resource. CVSS Rating: A:C

Vulnerability CVSS Score

Table 8. Dynamic Queueing System (DQS) message insertion CVSS score.

Scoring Date:	**N/A**	 **CVSS Calculator**
Base Score	**6.6**	
Impact Subscore	8.5	
Exploitability Subscore	4.9	
Temporal Score	**Not Defined**	
Overall Score	**6.6**	
		
Vector	(AV:N/AC:H/Au:N/C:P/I:P/A:C)	

5.1.5.11.1 Mitigations

Limiting what commands one service can insert into the queue of another (e.g., sending system shutdown commands from the ICCP service is probably unreasonable). Additionally, adding access controls to limit messages by user access level and client program would go a long way to mitigating this issue.

5.1.5.12 Zero-Day Vulnerability: Invalid Sized DQS Messages DoS

While fuzzing the DQS queue, a vulnerability was found that would cause some processes to crash. Sending DQS messages with zero or very high size fields triggered this issue. Not all processes were vulnerable. However, some processes, such as the *data_inp*, would cause the entire system to reboot if they crashed. This effect can be exploited to cause a DoS condition.

Retesting this vulnerability was done with the proof-of-concept code from Phase 1. Invalid sized messages still trigger this issue; therefore, this vulnerability is confirmed to still exist.

5.1.5.12.1 CVSS Base Metrics

Access Vector (AV)

The DQS queue can be accessed from less privileged systems.

The CVSS Access Vector rating is Network (N)—A vulnerability exploitable with network access means the vulnerable software is bound to the network stack, and the attacker does not require local network access or local access. Such a vulnerability is often termed “remotely exploitable.” CVSS Rating: AV:N

Access Complexity (AC)

An attacker would need to discover the DQS queue, services that use it, and begin fuzzing against them.

The CVSS Access Complexity rating is Medium (M); access conditions are somewhat specialized. CVSS Rating: AC:M

Authentication (Au)

No authentication is required to inject messages into the DQS queue.

The CVSS Authentication rating is None (N); authentication is not required to access and exploit the vulnerability. CVSS Rating: Au:N

Confidentiality Impact (C)

The CVSS Confidentiality Impact rating is None (N); there is no impact to the confidentiality of the system. CVSS Rating: C:N

Integrity Impact (I)

The CVSS Integrity Impact rating is None (N); there is no impact to the integrity of the system. CVSS Rating: I:N

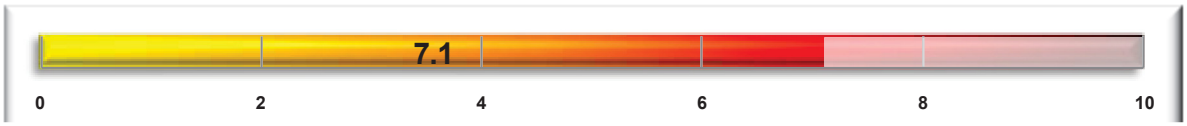
Availability Impact (A)

Causing certain services to crash can bring down the entire system (see: data_inp).

The CVSS Availability Impact rating is Complete (C); there is a total shutdown of the affected resource. CVSS Rating: A:C

Vulnerability CVSS Score

Table 9. Invalid sized DQS messages CVSS score.

Scoring Date:	**N/A**	 **CVSS Calculator**
Base Score	**7.1**	
Impact Subscore	6.9	
Exploitability Subscore	8.6	
Temporal Score	**Not Defined**	
Overall Score	**7.1**	
		
Vector	(AV:N/AC:M/Au:N/C:N/I:N/A:C)	

5.1.5.12.1 Mitigations

Implement improved error handling for invalid DQS messages (i.e., log the error and continue).

5.1.5.13 Zero-Day Vulnerability: ASUP DoS

Related to the DQS queue, the *ASUP* program accepts DQS messages to add or delete alarms from the system. The vulnerability was found when a message was sent to remove an alarm outside of the index of existing alarms. The ASUP program does not check for the validity of the index, and crashes as a result. This vulnerability can be exploited to create a DoS condition.

Source code review indicates that the vulnerability still exists; however, researchers were unable to trigger the vulnerability in this phase of testing. The array that is indexed has a size determined at compile time by a global variable. Researchers were unable to identify the value used for that variable. It is quite possible that the value was increased sufficiently invalidating the specific conditions required for attack.

5.1.5.13.1 CVSS Base Metrics

Access Vector (AV)

The DQS queue is accessible from less privileged systems.

The CVSS Access Vector rating is Network (N)—A vulnerability exploitable with network access means the vulnerable software is bound to the network stack, and the attacker does not require local network access or local access. Such a vulnerability is often termed “remotely exploitable.” CVSS Rating: AV:N

Access Complexity (AC)

An attacker would have to discover the DQS queue, the ASUP program, and its use thereof, and begin fuzzing the ASUP program.

The CVSS Access Complexity rating is Medium (M); access conditions are somewhat specialized. CVSS Rating: AC:M

Authentication (Au)

No authentication is required to inject messages into the DQS queue.

The CVSS Authentication rating is None (N); authentication is not required to access and exploit the vulnerability. CVSS Rating: Au:N

Confidentiality Impact (C)

The CVSS Confidentiality Impact rating is None (N); there is no impact to the confidentiality of the system. CVSS Rating: C:N

Integrity Impact (I)

The CVSS Integrity Impact rating is None (N); there is no impact to the integrity of the system. CVSS Rating: I:N

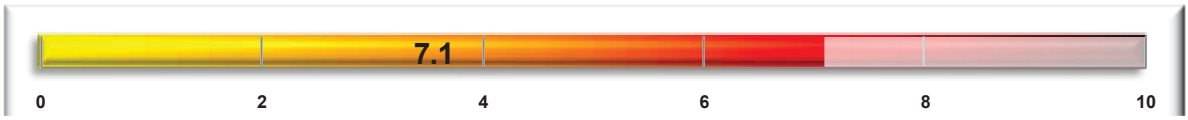
Availability Impact (A)

This attack can create a DoS condition by repeatedly crashing the ASUP program.

The CVSS Availability Impact rating is Complete (C); there is a total shutdown of the affected resource. CVSS Rating: A:C

Vulnerability CVSS Score

Table 10. ASUP DoS CVSS score.

Scoring Date:	**N/A**	 **CVSS Calculator**
Base Score	**7.1**	
Impact Subscore	6.9	
Exploitability Subscore	8.6	
Temporal Score	**Not Defined**	
Overall Score	**7.1**	
		
Vector	(AV:N/AC:M/Au:N/C:N/I:N/A:C)	

5.1.5.13.1 Mitigations

Error checking should be added to the ASUP program (and any others that use index values in DQS messages) to ensure that the index is valid. Should another program have this vulnerability and allow write-access, a remote code execution condition may exist.

5.1.5.14 Zero-Day Vulnerability: ICS Protocol Heap-based Overflow

The ICS protocol is used to send data from several other protocols across the system network. The ICS protocol is used on nearly every system in the Power TG network. While fuzzing the protocol, a heap-based overflow was found in the *ics_rbufget* function in the protocol-handling library. The ICS handler takes two different length fields from incoming packets to determine the internal buffer size and the amount to copy, allowing an attacker to overrun the buffer.

Source code was inspected to verify this vulnerability still exists for Phase 2.

5.1.5.14.1 CVSS Base Metrics

Access Vector (AV)

Processes that accept ICS messages are available on less-trusted systems.

The CVSS Access Vector rating is Network (N)—A vulnerability exploitable with network access means the vulnerable software is bound to the network stack, and the attacker does not require local network access or local access. Such a vulnerability is often termed “remotely exploitable.” CVSS Rating: AV:N

Access Complexity (AC)

An attacker would have to do significant work to reverse engineer the ICS protocol and craft an exploit for this vulnerability.

The CVSS Access Complexity rating is High (H); specialized access conditions exist. CVSS Rating: AC:H

Authentication (Au)

No authentication is required to send messages using the ICS transport protocol.

The CVSS authentication rating is None (N); authentication is not required to access and exploit the vulnerability. CVSS Rating: Au:N

Confidentiality Impact (C)

The attacker would be able to execute arbitrary code on the affected systems.

The CVSS Confidentiality Impact rating is Complete (C); there is a total information disclosure, resulting in all system files being revealed. Rating C:C

Integrity Impact (I)

An attacker would be able to gain control over any of the processes that handle ICS messages.

The CVSS Integrity Impact rating is Complete (C); there is a total compromise of system integrity. CVSS Rating: I:C

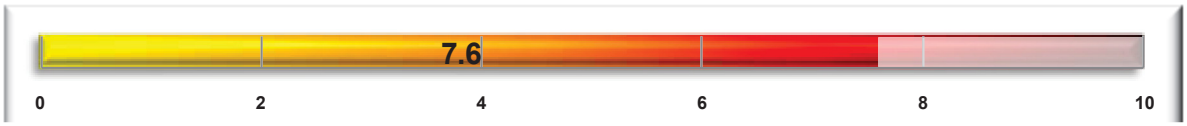
Availability Impact (A)

A successful buffer overflow would result in remote code execution and control of the system.

The CVSS Availability Impact rating is Complete (C); there is a total shutdown of the affected resource. CVSS Rating: A:C

Vulnerability CVSS Score

Table 11. ICS protocol heap-based overflow CVSS score.

Scoring Date:	**N/A**	 **CVSS Calculator**
Base Score	**7.6**	
Impact Subscore	10	
Exploitability Subscore	4.9	
Temporal Score	**Not Defined**	
Overall Score	**7.6**	
		
Vector	(AV:N/AC:H/Au:N/C:C/I:C/A:C)	

5.1.5.14.1 Mitigations

Implement bounds checking to ensure that the ICS handler does not overrun its internal buffer. Additionally, removing the second length field or ensuring that both length fields are equal would mitigate this vulnerability.

5.1.5.15 Zero-Day Vulnerability: Data_inp Global Buffer Overflow

The *data_inp* process is responsible for communications between the EMS server and the RTUCS. A potential buffer overflow was found in the "transparent" function within the *data_inp* process. This function copies data from the input packet into a global buffer, but does not confirm that the buffer is large enough to hold the data.

This vulnerability was verified again through source code review.

5.1.5.15.1 CVSS Base Metrics

Access Vector (AV)

Access to the network containing the EMS system is all that is required.

The CVSS Access Vector rating is Network (N)—A vulnerability exploitable with network access means the vulnerable software is bound to the network stack, and the attacker does not require local network access or local access. Such a vulnerability is often termed "remotely exploitable." CVSS Rating: AV:N

Access Complexity (AC)

Significant error is required to discover and exploit this vulnerability.

The CVSS Access Complexity rating is High (H); specialized access conditions exist. CVSS Rating: AC:H

Authentication (Au)

No authentication is required to communicate with the EMS server through this link.

The CVSS Authentication rating is None (N); authentication is not required to access and exploit the vulnerability. CVSS Rating: Au:N

Confidentiality Impact (C)

Arbitrary code execution would allow the attacker to access any available data on the affected system.

The CVSS Confidentiality Impact rating is Complete (C); there is a total information disclosure, resulting in all system files being revealed. Rating C:C

Integrity Impact (I)

Arbitrary code execution would allow the attacker to access any available data on the affected system.

The CVSS Integrity Impact rating is Complete (C); there is a total compromise of system integrity. CVSS Rating: I:C

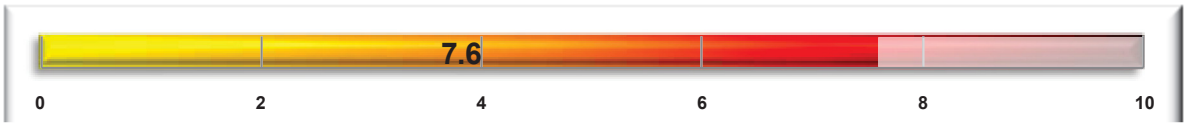
Availability Impact (A)

An attacker would be able to execute arbitrary code, as well as shut down the affected service.

The CVSS Availability Impact rating is Complete (C); there is a total shutdown of the affected resource. CVSS Rating: A:C

Vulnerability CVSS Score

Table 12. Data_inp global buffer overflow CVSS score.

Scoring Date:	**N/A**	 CVSS Calculator
Base Score	**7.6**	
Impact Subscore	10	
Exploitability Subscore	4.9	
Temporal Score	**Not Defined**	
Overall Score	**7.6**	
		
Vector	(AV:N/AC:H/Au:N/C:C/I:C/A:C)	

5.1.5.15.1 Mitigations

To mitigate this vulnerability, incoming network data should be checking for integrity, and bounds-checking should be implemented to ensure that data does not overrun the buffer.

5.1.5.16 Zero-Day Vulnerability: TG_RSH Stack-based Buffer Overflow

The *TG_RSH* program (and associated server daemon: *tg_rshserver*) is a custom variant of the Remote Shell (RSH) application. This program is used within the Power TG system to allow trusted computers to send commands to each other. This application is available on every server in the Power TG system. Reverse engineering led to the discovery of a stack-based overflow present in the "Xtun" function of the *tg_rshserver* program. This function reads a packet directly off the network and attempts to store it in a statically sized buffer. No checks are done to ensure that the data will fit within the buffer.

This vulnerability was verified again using the same techniques as Phase 1, assuming the Power TG Security Package was disabled. Phase 2's deployment featured additional security precautions that prevented the direct exploitation of this vulnerability, but a Power TG deployment would require the optional security package to help mitigate this vulnerability. However, this only prevents untrusted hosts from attempting this attack. The vulnerability can still be exploited from a trusted computer on the Power TG network, since a valid certificate is all that is needed to bypass the security checks. The CVSS score below is computed assuming the security package is not installed.

5.1.5.16.1 CVSS Base Metrics

Access Vector (AV)

An attacker would only need network access to any of the Power TG servers, as they all host the tg_rshserver process.

The CVSS Access Vector rating is Network (N)—A vulnerability exploitable with network access means the vulnerable software is bound to the network stack, and the attacker does not require local network access or local access. Such a vulnerability is often termed "remotely exploitable." CVSS Rating: AV:N

Access Complexity (AC)

This vulnerability could likely be discovered through fuzzing alone, although reverse engineering techniques were used.

The CVSS Access Complexity rating is Medium (M); access conditions are somewhat specialized. CVSS Rating: AC:M

Authentication (Au)

If the optional security package is installed, a single authentication step via Secure Socket Layer (SSL) certificate is required. However, the default (without optional components) installation of the Power TG system does not require authentication.

The CVSS Authentication rating is None (N); authentication is not required to access and exploit the vulnerability. CVSS Rating: Au:N

Confidentiality Impact (C)

Full system access would result from exploitation of this vulnerability.

The CVSS Confidentiality Impact rating is Complete (C); there is a total information disclosure, resulting in all system files being revealed. Rating C:C

Integrity Impact (I)

An attacker would gain the ability to execute arbitrary code on the compromised system.

The CVSS Integrity Impact rating is Complete (C); there is a total compromise of system integrity. CVSS Rating: I:C

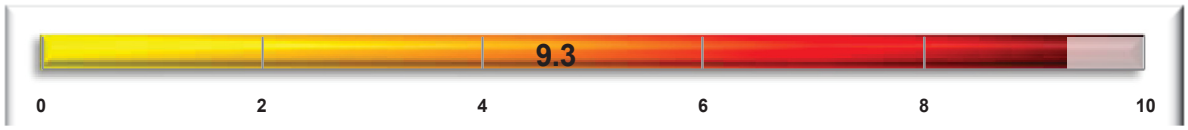
Availability Impact (A)

Compromise of the TG_RSH application can give an attacker control over any server in the Power TG system.

The CVSS Availability Impact rating is Complete (C); there is a total shutdown of the affected resource. CVSS Rating: A:C

Vulnerability CVSS Score

Table 13. TG_RSH stack-based buffer overflow CVSS score.

Scoring Date:	**N/A**	
Base Score	**9.3**	
Impact Subscore	10	
Exploitability Subscore	8.6	
Temporal Score	**Not Defined**	**CVSS Calculator**
Overall Score	**9.3**	
		
Vector	(AV:N/AC:M/Au:N/C:C/I:C/A:C)	

5.1.5.16.1 Mitigations

Implementing bounds-checking logic would mitigate this vulnerability. Incoming network data should be checked for integrity and consistency before being executed upon.

5.1.5.17 Resolved Zero-Day Vulnerability: DNP Fragment Reassembly Buffer Overflow

The Distributed Network Protocol (DNP) 3.0 is used to transmit data and commands between the RTU and the RTUCS. In Phase 1, a DNP fuzzer was used to test the RTUCS processes (*dnprsdd_driver*, *dnp_protocol_logic*, and *dnp_scan_results*) that handle DNP messages. One of the vulnerabilities found was a buffer overflow in the fragment reassembly logic.

For Phase 2, a DNP fuzzer was used to test this vulnerability again. Attempts to send messages in sizes ranging from 3,000 bytes to 17,000 bytes were done, but no overflow was detected. Although this vulnerability was not reproduced, this does not prove that the vulnerability does not exist.

5.1.5.17.1 Resolution

The protocol no longer crashes from a buffer overflow when given an overly large application data message sent in fragments.

5.1.5.18 Resolved Zero-Day Vulnerability: Large Invalid Ranges DoS

Another vulnerability was discovered while fuzzing the DNP handling processes by sending a range value indicating that many packets would be sent, but only sending a few (i.e., sending 100 packets with a range header indicating 10,000 would be sent). The vulnerability did not appear to allow for code execution, but caused the *dnp_scan_results* process to crash. The process would attempt to keep parsing data until it crashed.

In Phase 2, a DNP fuzzer was used to attempt to reproduce this issue. Sending messages with invalid range or count fields had no effect on the *dnp_scan_results* process, and the RTUCS would merely resend its data request in response. This vulnerability is considered resolved.

5.1.5.18.1 Resolution

The *dnp_scan_results* process no longer crashes when given an invalid range or count field. Instead, the RTUCS resends its data request.

5.1.5.19 Zero-Day Vulnerability: CREATE_GROUP Large object_count DoS

When sending a CREATE_GROUP message to the *api_server*, a crash can be caused by sending an overly large object_count message with no objects attached. This vulnerability can be exploited to cause a DoS condition by repeatedly crashing the *api_server* with malicious CREATE_GROUP messages. This vulnerability was reconfirmed in Phase 2 by source code review.

5.1.5.19.1 CVSS Base Metrics

Access Vector (AV)

This process does not require local or adjacent access to exploit.

The CVSS Access Vector rating is Network (N)—A vulnerability exploitable with network access means the vulnerable software is bound to the network stack, and the attacker does not require local network access or local access. Such a vulnerability is often termed "remotely exploitable." CVSS Rating: AV:N

Access Complexity (AC)

An attacker would be able to exploit this vulnerability with fuzzing alone, most likely.

The CVSS Access Complexity rating is Low (L); specialized access conditions or extenuating circumstances do not exist. CVSS Rating: AC:L

Authentication (Au)

No authentication is required to send messages to the *api_server* process.

The CVSS Authentication rating is None (N); authentication is not required to access and exploit the vulnerability. CVSS Rating: Au:N

Confidentiality Impact (C)

The CVSS Confidentiality Impact rating is None (N); there is no impact to the confidentiality of the system. CVSS Rating: C:N

Integrity Impact (I)

The CVSS Integrity Impact rating is None (N); there is no impact to the integrity of the system. CVSS Rating: I:N

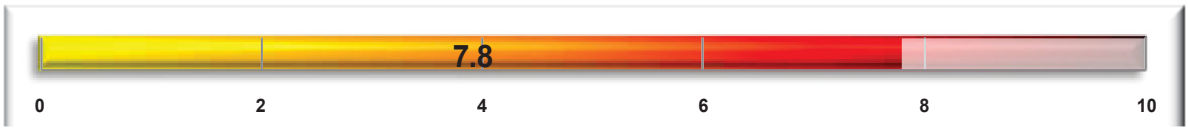
Availability Impact (A)

A DoS attack with this exploit would cause a total shutdown of the *api_server*.

The CVSS Availability Impact rating is Complete (C); there is a total shutdown of the affected resource. CVSS Rating: A:C

Vulnerability CVSS Score

Table 14. CREATE_GROUP large object_count DoS CVSS score.

Scoring Date:	**N/A**	 **CVSS Calculator**
Base Score	**7.8**	
Impact Subscore	6.9	
Exploitability Subscore	10	
Temporal Score	**Not Defined**	
Overall Score	**7.8**	
		
Vector	(AV:N/AC:L/Au:N/C:N/I:N/A:C)	

5.1.5.19.1 Mitigations

Add additional error checking to ensure that the object_count specified with the CREATE_GROUP message specifies a message that can fit within the receive buffer.

5.1.5.20 Zero-Day Vulnerability: CREATE_GROUP Large Name Stack-based Buffer Overflow

When a CREATE_GROUP message is sent to the *api_server* with a very large number of names in the payload, the *api_server* will crash due to a stack-based buffer overflow. The *api_server* does not ensure that the incoming names will fit within the static buffer allocated for them. This vulnerability was verified again through source code analysis.

5.1.5.20.1 CVSS Base Metrics

Access Vector (AV)

This process does not require local or adjacent access to exploit.

The CVSS Access Vector rating is Network (N)—A vulnerability exploitable with network access means the vulnerable software is bound to the network stack, and the attacker does not require local

network access or local access. Such a vulnerability is often termed “remotely exploitable.” CVSS Rating: AV:N

Access Complexity (AC)

This vulnerability could likely be exploited through simple fuzzing.

The CVSS Access Complexity rating is Low (L); specialized access conditions or extenuating circumstances do not exist. CVSS Rating: AC:L

Authentication (Au)

No authentication is required to send messages to the *api_server*.

The CVSS Authentication rating is None (N); authentication is not required to access and exploit the vulnerability. CVSS Rating: Au:N

Confidentiality Impact (C)

The CVSS Confidentiality Impact rating is None (N); there is no impact to the confidentiality of the system. CVSS Rating: C:N

Integrity Impact (I)

The CVSS Integrity Impact rating is None (N); there is no impact to the integrity of the system. CVSS Rating: I:N

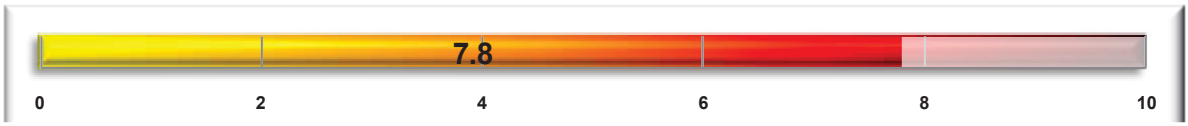
Availability Impact (A)

This vulnerability can be used to create a DoS condition, causing complete shutdown of the *api_server*.

The CVSS Availability Impact rating is Complete (C); there is a total shutdown of the affected resource. CVSS Rating: A:C

Vulnerability CVSS Score

Table 15. CREATE_GROUP large number of names DoS CVSS score.

Scoring Date:	**N/A**	 **CVSS Calculator**
Base Score	**7.8**	
Impact Subscore	6.9	
Exploitability Subscore	10	
Temporal Score	**Not Defined**	
Overall Score	**7.8**	
		
Vector	(AV:N/AC:L/Au:N/C:N/I:N/A:C)	

5.1.5.20.1 Mitigations

Add bounds-checking to ensure that the allocated buffer is large enough for the incoming payload.

5.1.5.21 CREATE_GROUP Large Name Stack-based Buffer Overflow

When a single name with more than 80 characters is sent in the CREATE_GROUP message's name payload the *api_server* crashes due to a stack-based buffer overflow. This overflow was found to corrupt the Extended Instruction Pointer (EIP), indicating the ability to inject and execute arbitrary code. This vulnerability was verified again through source code analysis.

5.1.5.21.1 CVSS Base Metrics

Access Vector (AV)

No local or adjacent network access is required to exploit this vulnerability.

The CVSS Access Vector rating is Network (N)—A vulnerability exploitable with network access means the vulnerable software is bound to the network stack, and the attacker does not require local network access or local access. Such a vulnerability is often termed "remotely exploitable." CVSS Rating: AV:N

Access Complexity (AC)

Simple fuzzing would lead to the discovery of this vulnerability. However, an exploit would still have to be crafted for the Power TG system.

The CVSS Access Complexity rating is Medium (M); access conditions are somewhat specialized. CVSS Rating: AC:M

Authentication (Au)

No authentication is required to send messages to the *api_server* process.

The CVSS Authentication rating is None (N); authentication is not required to access and exploit the vulnerability. CVSS Rating: Au:N

Confidentiality Impact (C)

Unlike Phase 1, this process no longer runs with administrative privileges, which limits the impact of this exploit somewhat.

The CVSS Confidentiality Impact rating is Partial (P); there is considerable informational disclosure. Rating C:P

Integrity Impact (I)

Arbitrary code execution gives the attacker the ability to compromise this process completely.

The CVSS Integrity Impact rating is Complete (C); there is a total compromise of system integrity. CVSS Rating: I:C

Availability Impact (A)

An attacker would get arbitrary code execution through this vulnerability, allowing them to shut down the resource.

The CVSS Availability Impact rating is Complete (C); there is a total shutdown of the affected resource. CVSS Rating: A:C

Vulnerability CVSS Score

Table 16. CREATE_GROUP large name stack-based buffer overflow CVSS score.

Scoring Date:	**N/A**	 CVSS Calculator
Base Score	**9**	
Impact Subscore	9.5	
Exploitability Subscore	8.6	
Temporal Score	**Not Defined**	
Overall Score	**9**	
		
Vector	(AV:N/AC:M/Au:N/C:P/I:C/A:C)	

5.1.5.21.1 Mitigations

Additional error handling should be added to reject or truncate CREATE_GROUP message payloads with overly large names.

5.1.6 Conclusions

Numerous vulnerabilities to the Siemens Power TG system were found in Phase 1 of this assessment. Many were configuration-related issues that could be resolved in a reasonable amount of time. Others were process-specific vulnerabilities (buffer overflows, etc.) that allowed a DoS or remote code execution condition to exist. Some of these have been resolved, but others remain that could cause partial or full system compromise if found and exploited. Of the twenty-three vulnerabilities retested, eight (35 percent) have been resolved and fifteen (65 percent) are still vulnerable. The majority of these vulnerabilities could be resolved by implementing proper bounds-checking and better integrity checking for network traffic being processed.

Due to technical difficulties and time constraints, some of the original targets were not tested. Since the ICCP and Historian systems could not be retested, is it currently unknown whether their vulnerabilities still exist.

5.2 Target 2 – Primary Server

5.2.1 Introduction

This assessment target assessed processes, connections, etc., on the primary server (host) in the Siemens Power TG system for exploitable vulnerabilities.

This section attempts to extract the pertinent information from the Cyber Researcher's report on AT2. The Cyber Researcher's report documents to a level where "someone similarly skilled in the art" can reproduce the results. This level is not required for the general report. For the reader that needs this level of detail, read the attached Cyber Researcher's report: Siemens Spectrum Power TG Cyber Report for AT2 – Primary Server.

5.2.2 Objective

The objective of this assessment target is to assess the TG primary server for vulnerabilities that may allow unauthorized access to the primary server or disrupt the TG system. This objective has a specific goal of compromising the primary server or the TG system through its network services. The test system has a primary server and a hot standby primary server; both are targets.

5.2.3 Significance

As the name indicates, the TG primary server is the center of the TG system. The primary server holds the system configuration database, used to configure the TG system, including security settings. The primary server also maintains the real-time database, which is updated with field data from the RTUCS and used to update the operator's workstation, Web HMI server, and other EMS processes. The ability to alter data to or from either of these databases could have serious consequences. Disruption of primary server services could affect the entire TG system.

5.2.4 Rules of Engagement

There were no rules of engagement that impacted this portion of the assessment.

5.2.5 Assessment

Also referred to as the Primary and Standby Databases, the primary servers can be Microsoft or Linux based. The most common is a Linux operating system. Redhat 4.8 is implemented in the test system. These two nodes have additional network interfaces used to pass data and perform watchdog checks for failover. The process information is fed to both of these nodes at the same time. They stay in lock-step because that data is sent to both systems (databases). They have an ODBC link to an archive that allows archiving of process data. In addition, there can be a third database called the EBS. Once the initial download is completed, this database server just listens to traffic and can be manually shifted to by the operator. It does not automatically become a primary database. The EBS can be placed in the Demilitarized Zone (DMZ), segregated by a firewall from the control network.

The primary server maintains the real-time database and is the center of the TG system.

5.2.5.1 Method 1: Source Code Review

The method of source code review is primarily one of identifying code within a process that handles or interacts with user-supplied data. From there it is a matter of working through how that data is used by the process, and what a user (or attacker) can do to influence or corrupt the processes.

In many cases, source code review can be detrimental to the overall goal of identifying vulnerabilities, as the amount of time it takes to become familiar with the development environment and conventions used by developers may be prohibitive.

With the Siemens TG system, the source code provided as a standard part of the Linux installation proved to be clear enough to allow for relatively quick understanding.

5.2.5.2 Vulnerability: Heap-based Buffer Overflow in TG RSH Server rcpdb_expand Function

A heap-based buffer overflow[7] vulnerability exists in the tg_rshserver rcpdb_expand() function of the TG RSH server which runs on all TG hosts.

5.2.5.2.1 CVSS Base Metrics

Access Vector (AV)

The CVSS Access Vector rating is Network (N)—A vulnerability exploitable with network access means the vulnerable software is bound to the network stack, and the attacker does not require local network access or local access. Such a vulnerability is often termed "remotely exploitable." CVSS Rating: AV:N

Access Complexity (AC)

Depending on system configuration, the complexity of gaining access to exploit the TG RSH server buffer overflow ranges from performing a simple DNS spoof attack to bypassing SSL authentication.

The CVSS Access Complexity rating is Medium (M); access conditions are somewhat specialized. CVSS Rating: AC:M

Authentication (Au)

The Authentication rating for this vulnerability is None because the default system does not require an attacker to provide credentials before an exploit may occur.

The CVSS Authentication rating is None (N); authentication is not required to access and exploit the vulnerability. CVSS Rating: Au:N

Confidentiality Impact (C)

The CVSS Confidentiality Impact rating is None (N); there is no impact to the confidentiality of the system. CVSS Rating: C:N

---

7. "A heap overflow condition is a buffer overflow, where the buffer that can be overwritten is allocated in the heap portion of memory, generally meaning that the buffer was allocated using a routine such as `malloc()`." http://cwe.mitre.org/data/definitions/122.html

Integrity Impact (I)

The CVSS Integrity Impact rating is None (N); there is no impact to the integrity of the system. CVSS Rating: I:N

Availability Impact (A)

This vulnerability can be exploited to crash the TG RSH server, rendering that service unavailable.

The CVSS Availability Impact rating is Complete (C); there is a total shutdown of the affected resource. CVSS Rating: A:C

Vulnerability CVSS Score

Table 17. Heap-based buffer overflow in TG RSH Server rcpdb_expand function CVSS score.

Scoring Date:	**N/A**	 **CVSalculator**
Base Score	**7.1**	
Impact Subscore	6.9	
Exploitability Subscore	8.6	
Temporal Score	**Not Defined**	
Overall Score	**7.1**	
		
Vector	(AV:N/AC:M/Au:N/C:N/I:N/A:C)	

5.2.5.2.1 Mitigations

The `Blocksize` value should be validated before it is used in the `memcpy()` function.

5.2.5.3 Vulnerability: Unchecked Input for Loop Condition in TG RSH Server tg_rshserver_dbcopy Function

An unchecked input for loop condition[8] vulnerability exists in the `tg_rshserver_dbcopy()` function. The TG RSH server runs on all TG hosts.

A DoS condition or possibly remote code execution may occur if an attacker is able to send a specially crafted database block to the TG RSH server.

8. "The product does not properly check inputs that are used for loop conditions, potentially leading to a denial of service because of excessive looping." http://cwe.mitre.org/data/definitions/606.html

5.2.5.3.1 CVSS Base Metrics

Access Vector (AV)

The CVSS Access Vector rating is Network (N)—A vulnerability exploitable with network access means the vulnerable software is bound to the network stack, and the attacker does not require local network access or local access. Such a vulnerability is often termed "remotely exploitable." CVSS Rating: AV:N

Access Complexity (AC)

Depending on system configuration, the complexity of gaining access to exploit the TG RSH server buffer overflow ranges from performing a simple DNS spoof attack to bypassing SSL authentication.

The CVSS Access Complexity rating is Medium (M); access conditions are somewhat specialized. CVSS Rating: AC:M

Authentication (Au)

The Authentication rating for this vulnerability is None because the default system does not require an attacker to provide credentials before an exploit may occur.

The CVSS Authentication rating is None (N); authentication is not required to access and exploit the vulnerability. CVSS Rating: Au:N

Confidentiality Impact (C)

The team proved exploitability of the heap-based buffer overflow, but did not create a complete exploit to gain remote code execution. It is possible that an attacker can exploit this vulnerability to gain access to the Primary Host as root. (The TG RSH server has the setuid bit set and runs as root.) Vulnerabilities that give root-level access should be scored with complete loss of confidentiality, integrity, and availability.

The CVSS Confidentiality Impact rating is Complete (C); there is a total information disclosure, resulting in all system files being revealed. Rating C:C

Integrity Impact (I)

An attacker may be able to exploit this vulnerability to gain root access to the Primary Host.

The CVSS Integrity Impact rating is Complete (C); there is a total compromise of system integrity. CVSS Rating: I:C

Availability Impact (A)

This vulnerability can be exploited to crash the TG RSH server, rendering that service unavailable.

The CVSS Availability Impact rating is Complete (C); there is a total shutdown of the affected resource. CVSS Rating: A:C

Vulnerability CVSS Score

Table 18. Unchecked input for loop condition in TG RSH Server tg_rshserver_dbcopy function CVSS score.

Scoring Date:	**N/A**	 **CVSS Calculator**
Base Score	**9.3**	
Impact Subscore	10	
Exploitability Subscore	8.6	
Temporal Score	**Not Defined**	
Overall Score	**9.3**	
		
Vector	(AV:N/AC:M/Au:N/C:C/I:C/A:C)	

5.2.5.3.1 Mitigations

Perform input validation of the num_dbfiles variable before it is used. It is recommended not to use user-controlled data for loop conditions. If user-controlled data is used for loop conditions, it should be validated.

5.2.5.4 Vulnerability: Stack-based Buffer Overflow in TG RSH Server pcs_create_sem_pl Function

A stack-based buffer overflow[9] vulnerability exists in the `pcs_create_sem_pl()` function of the tg_rshserver service, which is available on the Primary Hosts, as well as the other TG hosts. This vulnerability could allow a user to gain root access.

5.2.5.4.1 CVSS Base Metrics

Access Vector (AV)

Local access or access to a shell account on the host is required to start the tg_rshserver process.

The CVSS Access Vector rating is Local (L)—A vulnerability exploitable with only *local access* requires the attacker to have either physical access to the vulnerable system or a local (shell) account. CVSS Rating: AV:L

9. "A stack-based buffer overflow condition is a condition where the buffer being overwritten is allocated on the stack (i.e., is a local variable or, rarely, a parameter to a function)." http://cwe.mitre.org/data/definitions/121.html

Access Complexity (AC)

Once local access to the host is obtained, no special circumstances are required to exploit this vulnerability.

The CVSS Access Complexity rating is Low (L); specialized access conditions or extenuating circumstances do not exist. CVSS Rating: AC:L

Authentication (Au)

No authentication is required to execute the tg_rshserver process once local access to the host has been obtained.

The CVSS Authentication rating is Single (S); one instance of authentication is required to access and exploit the vulnerability. CVSS Rating: Au:S

Confidentiality Impact (C)

This buffer overflow vulnerability can be exploited to escalate privileges to root access. The attacker is able to read all of the system's data (memory, files, etc.)

The CVSS Confidentiality Impact rating is Complete (C); there is a total information disclosure, resulting in all system files being revealed. Rating C:C

Integrity Impact (I)

There is a complete loss of system protection, resulting in the entire system being compromised. The attacker is able to modify any files on the target system.

The CVSS Integrity Impact rating is Complete (C); there is a total compromise of system integrity. CVSS Rating: I:C

Availability Impact (A)

The attacker can render the resource completely unavailable.

The CVSS Availability Impact rating is Complete (C); there is a total shutdown of the affected resource. CVSS Rating: A:C

Vulnerability CVSS Score

Table 19. Stack-based buffer overflow in TG RSH Server pcs_create_sem_pl function CVSS score.

Scoring Date:	**N/A**	 **CVSS Calculator**
Base Score	**6.8**	
Impact Subscore	10	
Exploitability Subscore	3.1	
Temporal Score	**Not Defined**	
Overall Score	**6.8**	
		
Vector	(AV:L/AC:L/Au:S/C:C/I:C/A:C)	

5.2.5.4.1 Mitigations

Code that requires setuid should be thoroughly evaluated for buffer overflow vulnerabilities and all buffer overflow vulnerabilities should be remediated.

5.2.5.5 Vulnerability: Unchecked Input for Loop Condition in API Server apisrv_emsproc_nbr Function

An unchecked input for loop condition vulnerability exists in the API server `apisrv_emsproc_nbr()` function, defined in apisrvemsproc.c.

A crash or DoS of the API server may occur if it is sent client requests with invalid values for `name_count` or `emsproc_names`.

5.2.5.5.1 CVSS Base Metrics

Access Vector (AV)

The CVSS Access Vector rating is Network (N)—A vulnerability exploitable with network access means the vulnerable software is bound to the network stack, and the attacker does not require local network access or local access. Such a vulnerability is often termed “remotely exploitable.” CVSS Rating: AV:N

Access Complexity (AC)

Depending on system configuration, the complexity of gaining access to exploit the TG API server buffer overflow ranges from performing a simple DNS spoof attack to bypassing SSL authentication.

The CVSS Access Complexity rating is Medium (M); access conditions are somewhat specialized. CVSS Rating: AC:M

Authentication (Au)

The Authentication rating for this vulnerability is None because the default system does not require an attacker to provide credentials before an exploit may occur.

The CVSS Authentication rating is None (N); authentication is not required to access and exploit the vulnerability. CVSS Rating: Au:N

Confidentiality Impact (C)

It is possible that an attacker can exploit this vulnerability to gain access to the Primary Host as the powertglocal user. Vulnerabilities that give user-level access should be scored with only partial loss of confidentiality, integrity, and availability.

The CVSS Confidentiality Impact rating is Partial (P); there is considerable informational disclosure. Rating C:P

Integrity Impact (I)

An attacker may be able to exploit this vulnerability to gain access to the Primary Host as the powertglocal user.

The CVSS Integrity Impact rating is Partial (P); modification of some system files or information is possible. CVSS Rating: I:P

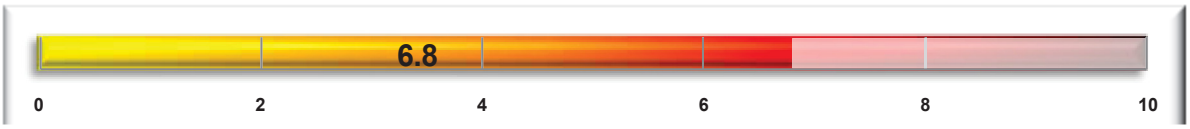
Availability Impact (A)

This vulnerability can be exploited to crash the TG API server, rendering that service unavailable.

The CVSS Availability Impact rating is Partial (P); there is reduced performance or interruptions in resource availability. CVSS Rating: A:P

Vulnerability CVSS Score

Table 20. Unchecked input for loop condition in API Server apisrv_emsproc_nbr function CVSS score.

Scoring Date:	**N/A**	 **CVSS Calculator**
Base Score	**6.8**	
Impact Subscore	6.4	
Exploitability Subscore	8.6	
Temporal Score	**Not Defined**	
Overall Score	**6.8**	
		
Vector	(AV:N/AC:M/Au:N/C:P/I:P/A:P)	

5.2.5.5.1 Mitigations

Perform input validation. It is recommended not to use user-controlled data for loop conditions. If user-controlled data is used for loop conditions, it should be validated.

5.2.5.6 Vulnerability: Stack-based Buffer Overflow in API Server API_TRACE_1 Macro

A stack-based buffer overflow vulnerability exists in the API server `apisrv_emsproc_nbr()` function when it calls the `API_TRACE_1` macro.

5.2.5.6.1 CVSS Base Metrics

Access Vector (AV)

The CVSS Access Vector rating is Network (N)—A vulnerability exploitable with network access means the vulnerable software is bound to the network stack, and the attacker does not require local network access or local access. Such a vulnerability is often termed "remotely exploitable." CVSS Rating: AV:N

Access Complexity (AC)

Depending on system configuration, the complexity of gaining access to exploit the TG API server buffer overflow ranges from performing a simple DNS spoof attack to bypassing SSL authentication.

The CVSS Access Complexity rating is Medium (M); access conditions are somewhat specialized. CVSS Rating: AC:M

Authentication (Au)

The Authentication rating for this vulnerability is None because the default system does not require an attacker to provide credentials before an exploit may occur.

The CVSS Authentication rating is None (N); authentication is not required to access and exploit the vulnerability. CVSS Rating: Au:N

Confidentiality Impact (C)

It is possible that an attacker can exploit this vulnerability to gain access to the Primary Host as the powertglocal user. Vulnerabilities that give user-level access should be scored with only partial loss of confidentiality, integrity, and availability.

The CVSS Confidentiality Impact rating is Partial (P); there is considerable informational disclosure. Rating C:P

Integrity Impact (I)

An attacker may be able to exploit this vulnerability to gain access to the Primary Host as the powertglocal user.

The CVSS Integrity Impact rating is Partial (P); modification of some system files or information is possible. CVSS Rating: I:P

Availability Impact (A)

This vulnerability can be exploited to crash the TG API server, rendering that service unavailable.

The CVSS Availability Impact rating is Partial (P); there is reduced performance or interruptions in resource availability. CVSS Rating: A:P

Vulnerability CVSS Score

Table 21. Stack-based buffer overflow in API Server API_TRACE_1 macro CVSS score.

Scoring Date:	**N/A**	 **CVSS Calculator**
Base Score	**6.8**	
Impact Subscore	6.4	
Exploitability Subscore	8.6	
Temporal Score	**Not Defined**	
Overall Score	**6.8**	
		
Vector	(AV:N/AC:M/Au:N/C:P/I:P/A:P)	

5.2.5.6.1 Mitigations

Perform input validation. The user-supplied input values should be checked to validate that they will fit within the input buffer before they are copied.

5.2.5.7 Vulnerability: Stack-based Buffer Overflow in API Server apisrv_write_rts_list Function

A buffer overflow vulnerability exists in the API server `apisrv_emsproc_nbr()` function, which is used to write messages into the alarm and event list.

5.2.5.7.1 CVSS Base Metrics

Access Vector (AV)

The CVSS Access Vector rating is Network (N)—A vulnerability exploitable with network access means the vulnerable software is bound to the network stack, and the attacker does not require local network access or local access. Such a vulnerability is often termed “remotely exploitable.” CVSS Rating: AV:N

Access Complexity (AC)

Depending on system configuration, the complexity of gaining access to exploit the TG API server buffer overflow ranges from performing a simple DNS spoof attack to bypassing SSL authentication.

The CVSS Access Complexity rating is Medium (M); access conditions are somewhat specialized. CVSS Rating: AC:M

Authentication (Au)

The Authentication rating for this vulnerability is None because the default system does not require an attacker to provide credentials before an exploit may occur.

The CVSS Authentication rating is None (N); authentication is not required to access and exploit the vulnerability. CVSS Rating: Au:N

Confidentiality Impact (C)

The Confidentiality metric measures the impact on confidentiality of a successfully exploited vulnerability. Confidentiality refers to limiting information access and disclosure to only authorized users, as well as preventing access by, or disclosure to, unauthorized ones.

It is possible that an attacker can exploit this vulnerability to gain access to the Primary Host as the powertglocal user. Vulnerabilities that give user-level access should be scored with only partial loss of confidentiality, integrity, and availability.

The CVSS Confidentiality Impact rating is Partial (P); considerable informational disclosure. Rating C:P

Integrity Impact (I)

An attacker may be able to exploit this vulnerability to gain access to the Primary Host as the powertglocal user.

The CVSS Integrity Impact rating is Partial (P); modification of some system files or information is possible. CVSS Rating: I:P

Availability Impact (A)

This vulnerability can be exploited to crash the TG API server, rendering that service unavailable.

The CVSS Availability Impact rating is Partial (P); reduced performance or interruptions in resource availability. CVSS Rating: A:P

Vulnerability CVSS Score

Table 22. Stack-based buffer overflow in API Server apisrv_write_rts_list function CVSS score.

Scoring Date:	**N/A**	 **CVSS Calculator**
Base Score	**6.8**	
Impact Subscore	6.4	
Exploitability Subscore	8.6	
Temporal Score	**Not Defined**	
Overall Score	**6.8**	
		
Vector	(AV:N/AC:M/Au:N/C:P/I:P/A:P)	

5.2.5.7.1 Mitigations

Perform input validation. The user-supplied input values should be checked to validate that they will fit within the input buffer before they are copied.

5.2.5.8 Vulnerability: Heap-based Buffer Overflow in API Server add_connection_cli Function

A buffer overflow vulnerability exists in the API server `add_connection_cli()` function.

5.2.5.8.1 CVSS Base Metrics

Access Vector (AV)

The CVSS Access Vector rating is Network (N)—A vulnerability exploitable with network access means the vulnerable software is bound to the network stack, and the attacker does not require local network access or local access. Such a vulnerability is often termed "remotely exploitable." CVSS Rating: AV:N

Access Complexity (AC)

Depending on system configuration, the complexity of gaining access to exploit the TG API server buffer overflow ranges from performing a simple DNS spoof attack to bypassing SSL authentication.

The CVSS Access Complexity rating is Medium (M); access conditions are somewhat specialized. CVSS Rating: AC:M

Authentication (Au)

The Authentication rating for this vulnerability is None because the default system does not require an attacker to provide credentials before an exploit may occur.

The CVSS Authentication rating is None (N); authentication is not required to access and exploit the vulnerability. CVSS Rating: Au:N

Confidentiality Impact (C)

It is possible that an attacker can exploit this vulnerability to gain access to the Primary Host as the powertglocal user. Vulnerabilities that give user-level access should be scored with only partial loss of confidentiality, integrity, and availability.

The CVSS Confidentiality Impact rating is Partial (P); there is considerable informational disclosure. Rating C:P

Integrity Impact (I)

An attacker may be able to exploit this vulnerability to gain access to the Primary Host as the powertglocal user.

The CVSS Integrity Impact rating is Partial (P); modification of some system files or information is possible. CVSS Rating: I:P

Availability Impact (A)

This vulnerability can be exploited to crash the TG API server, rendering that service unavailable.

The CVSS Availability Impact rating is Partial (P); there is reduced performance or interruptions in resource availability. CVSS Rating: A:P

Vulnerability CVSS Score

Table 23. Heap-based buffer overflow in API Server add_connection_cli function CVSS score.

Scoring Date:	**N/A**	 **CVSS Calculator**
Base Score	**6.8**	
Impact Subscore	6.4	
Exploitability Subscore	8.6	
Temporal Score	**Not Defined**	
Overall Score	**6.8**	
		
Vector	(AV:N/AC:M/Au:N/C:P/I:P/A:P)	

5.2.5.8.1 Mitigations

Perform input validation. The user-supplied input values should be checked to validate that they will fit within the input buffer before they are copied.

5.2.5.9 Vulnerability: Integer Overflow to Heap-based Buffer Overflow in RDBS Server

An integer overflow[10] to heap-based buffer overflow exists in the rdbs_server server application on the Primary and Hot Standby servers, inlhosta and inlhostb. The RDBS server writes data to the system database from a remote process.

5.2.5.9.1 CVSS Base Metrics

Access Vector (AV)

The CVSS Access Vector rating is Network (N)—A vulnerability exploitable with network access means the vulnerable software is bound to the network stack, and the attacker does not require local network access or local access. Such a vulnerability is often termed "remotely exploitable." CVSS Rating: AV:N

10. "The software performs a calculation that can produce an integer overflow or wraparound, when the logic assumes that the resulting value will always be larger than the original value...An integer overflow or wraparound occurs when an integer value is incremented to a value that is too large to store in the associated representation. When this occurs, the value may wrap to become a very small or negative number. While this may be intended behavior in circumstances that rely on wrapping, it can have security consequences if the wrap is unexpected. This is especially the case if the integer overflow can be triggered using user-supplied inputs. This becomes security-critical when the result is used to control looping, make a security decision, or determine the offset or size in behaviors such as memory allocation, copying, concatenation, etc." http://cwe.mitre.org/data/definitions/190.html

Access Complexity (AC)

Depending on system configuration, the complexity of gaining access to exploit the rdbs_server buffer overflow ranges from performing a simple DNS spoof attack to bypassing SSL authentication.

The CVSS Access Complexity rating is Medium (M); access conditions are somewhat specialized. CVSS Rating: AC:M

Authentication (Au)

The Authentication rating for this vulnerability is None because the default system does not require an attacker to provide credentials before an exploit may occur.

The CVSS Authentication rating is None (N); authentication is not required to access and exploit the vulnerability. CVSS Rating: Au:N

Confidentiality Impact (C)

Vulnerabilities that give user-level access should be scored with only partial loss of confidentiality, integrity, and availability.

The CVSS Confidentiality Impact rating is Partial (P); there is considerable informational disclosure. Rating C:P

Integrity Impact (I)

An attacker may be able to exploit this vulnerability to gain powertglocal user access to the Primary Host.

The CVSS Integrity Impact rating is Partial (P); modification of some system files or information is possible. CVSS Rating: I:P

Availability Impact (A)

This vulnerability can be exploited to crash the rdbs_server, rendering that service unavailable.

The CVSS Availability Impact rating is Partial (P); there is reduced performance or interruptions in resource availability. CVSS Rating: A:P

Vulnerability CVSS Score

Table 24. Integer overflow to heap-based buffer overflow in RDBS Server CVSS score.

Scoring Date:	**N/A**	 **CVSS Calculator**
Base Score	**6.8**	
Impact Subscore	6.4	
Exploitability Subscore	8.6	
Temporal Score	**Not Defined**	
Overall Score	**6.8**	
		
Vector	(AV:N/AC:M/Au:N/C:P/I:P/A:P)	

5.2.5.9.1 Mitigations

The rdbs_server code should implement bounds checking. An independent user-supplied length field should not be trusted. The input data should be validated before it is copied into memory. A check should be made to validate that the input data is actually the size specified. If the actual size differs from the length field, it should be dealt with appropriately.

5.2.5.10 Vulnerability: Buffer Overflow in ws_startup.exe

A buffer overflow vulnerability exists in the ws_startup process of the Primary Hosts, as well as the operator workstation, inlws01.

5.2.5.10.1 CVSS Base Metrics

Access Vector (AV)

Local access or access to a shell account on the host is required to start the ws_startup process.

The CVSS Access Vector rating is Local (L)—A vulnerability exploitable with only *local access* requires the attacker to have either physical access to the vulnerable system or a local (shell) account. CVSS Rating: AV:L

Access Complexity (AC)

Once local access to the host is obtained, no special circumstances are required to exploit this vulnerability.

The CVSS Access Complexity rating is Low (L); specialized access conditions or extenuating circumstances do not exist. CVSS Rating: AC:L

Authentication (Au)

No authentication is required to execute the ws_startup process once local access to the host has been obtained.

The CVSS Authentication rating is Single (S); one instance of authentication is required to access and exploit the vulnerability. CVSS Rating: Au:S

Confidentiality Impact (C)

This buffer overflow vulnerability can be exploited to escalate privileges to root access. The attacker is able to read all of the system's data (memory, files, etc.).

The CVSS Confidentiality Impact rating is Complete (C); there is a total information disclosure, resulting in all system files being revealed. Rating C:C

Integrity Impact (I)

There is a complete loss of system protection, resulting in the entire system being compromised. The attacker is able to modify any files on the target system.

The CVSS Integrity Impact rating is Complete (C); there is a total compromise of system integrity. CVSS Rating: I:C

Availability Impact (A)

The attacker can render the resource completely unavailable.

The CVSS Availability Impact rating is Complete (C); there is a total shutdown of the affected resource. CVSS Rating: A:C

Vulnerability CVSS Score

Table 25. Heap-based buffer overflow in ws_startup.exe CVSS score.

Scoring Date:	**N/A**	 **CVSS Calculator**
Base Score	**6.8**	
Impact Subscore	10	
Exploitability Subscore	3.1	
Temporal Score	**Not Defined**	
Overall Score	**6.8**	
		
Vector	(AV:L/AC:L/Au:S/C:C/I:C/A:C)	

5.2.5.10.1 Mitigations

Code that requires setuid should be thoroughly evaluated for buffer overflow vulnerabilities and all buffer overflow vulnerabilities should be remediated.

5.2.5.11 Vulnerability: Heap-based Buffer Overflow in Scriptlite Utility

A heap-based buffer overflow exists in the Scriptlite utility used to generate a ScriptCALC source file for a substation from the calculation definitions in the source database. The Scriptlite utility is available on the primary hosts.

5.2.5.11.1 CVSS Base Metrics

Access Vector (AV)

This vulnerability requires local access to a TG host with the Scriptlite utility.

The CVSS Access Vector rating is Local (L) - A vulnerability exploitable with only *local access* requires the attacker to have either physical access to the vulnerable system or a local (shell) account. CVSS Rating: AV:L

Access Complexity (AC)

Once local access to the operator workstation is obtained, no special circumstances are required to exploit this vulnerability.

The CVSS Access Complexity rating is Low (L); specialized access conditions or extenuating circumstances do not exist. CVSS Rating: AC:L

Authentication (Au)

An attacker must authenticate to the operating system as a user with permission to execute the Scriptlite utility before exploiting this vulnerability. The Scriptlite utility does not require authentication.

The CVSS Authentication rating is Single (S); one instance of authentication is required to access and exploit the vulnerability. CVSS Rating: Au:S

Confidentiality Impact (C)

The CVSS Confidentiality Impact rating is Partial (P); there is considerable informational disclosure. Rating C:P

Integrity Impact (I)

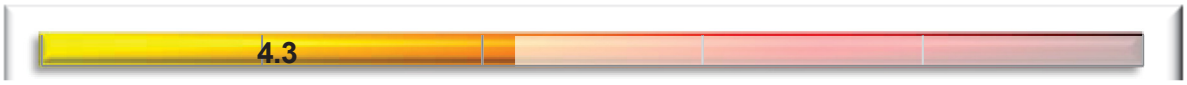
The CVSS Integrity Impact rating is Partial (P); modification of some system files or information is possible. CVSS Rating: I:P

Availability Impact (A)

The CVSS Availability Impact rating is Partial (P); there is reduced performance or interruptions in resource availability. CVSS Rating: A:P

Vulnerability CVSS Score

Table 26. Heap-based buffer overflow in Scriptlite utility CVSS score.

Scoring Date:	**N/A**	 **CVSS Calculator**
Base Score	**4.3**	
Impact Subscore	6.4	
Exploitability Subscore	3.1	
Temporal Score	**Not Defined**	
Overall Score	**4.3**	
		
Vector	(AV:L/AC:L/Au:S/C:P/I:P/A:P)	

5.2.5.11.1 Mitigations

Code that requires setuid should be thoroughly evaluated for buffer overflow vulnerabilities and all buffer overflow vulnerabilities should be remediated.

5.2.5.12 Method Conclusions

Code for the TG services and other executables available on the Primary and Hot Standby Hosts was evaluated for potential vulnerabilities, to the extent possible within the assessment timeframe.

Ten vulnerabilities were discovered: seven vulnerabilities were discovered that could allow a remote attacker to cause a DoS or gain access to the Primary or Hot Standby Host and three vulnerabilities that could allow a local user to escalate privileges.

It is recommended that these vulnerabilities be remediated with proper input validation and that the TG code base be further analyzed for additional vulnerabilities.

5.2.6 Conclusions

The objective of this assessment target was to assess the TG primary server for vulnerabilities that may allow unauthorized access to the primary server or disrupt the TG system. Ten vulnerabilities were discovered: seven vulnerabilities that could allow a remote attacker to cause a DoS or gain access to the Primary or Hot Standby Host and three vulnerabilities that could allow a local user to escalate privileges.

All of the vulnerabilities in this report are due to missing or inadequate input validation. The assessment team was not able to review all of the TG code. Siemens should review all code and make sure that all input is validated before it is used.

5.3 Target 3 – DQS Protocol Handling

5.3.1 Introduction

This assessment target focuses on the Siemens Power TG DQS protocol. The DQS protocol is used within the Siemens TG System to transmit data between processes, which can be running on a single host, or on multiple hosts interconnected through standard IP/Ethernet-based networks. DQS messages are one of the primary means of IPC on the Siemens Power TG system, carrying consumable control system data as well as command and control messages.

This section attempts to extract the pertinent information from the Cyber Researcher's report on AT3. The Cyber Researcher's report documents to a level where "someone similarly skilled in the art" can reproduce the results. This level is not required for the general report. For the reader that needs this level of detail, read the attached Cyber Researcher's report: Siemens Spectrum Power TG Cyber Report for AT3 – DQS Protocol.

5.3.2 Objective

The basic objective of this assessment target is to assess the DQS protocol. This objective is further broken down into two more specific areas that were evaluated. Namely, to evaluate an attacker's ability to use the DQS messaging mechanism to attack the overall Power TG system, and to evaluate an attackers ability to insert arbitrary DQS messages into the system message queue from an unprivileged position.

5.3.3 Significance

The DQS protocol is one of the primary means of IPC within the Siemens Power TG system. It carries messages dealing with basic data and control system information as well as command messages to

the system itself. If attackers were able to interact with the Power TG system through the DQS protocol, they would effectively have complete control of the system and the data it provides.

5.3.4 Rules of Engagement

The Siemens Power TG system has an optional security package, consisting of shared library containing an implementation of the OpenSSL[11] library. When the security system is not installed, a shared library consisting of stub functions is used and called by the system instead. Stub functions are small functions that act as placeholders for other, complete implementations. The test system at INL had the optional security package installed, and hosts were evaluated with and without the security library protections according to the specific goals and method of the test being performed.

The DQS protocol was looked at in Phase 1 of testing also performed at INL. Issues identified in Phase 1 were not explicitly tested in this Phase 2 assessment; however, where possible, results and information gained in Phase 1 were used to help expedite the work performed during this second round of testing.

5.3.5 Assessment

As stated in Section 5.3.2, there were two goals to assessing the DQS target: attacking the Power TG system (via its processes) through DQS messages, assessed through fuzzing,[12] and source code review of processes that handle DQS messages. The second goal, inserting arbitrary messages into the DQS queue, was assessed through reverse engineering of the optional security library. The researchers focused on the optional security package library for the second goal as the Phase 1 assessment had already demonstrated the ability to inject arbitrary DQS messages into the messaging queue without the security package installed.

5.3.5.1 Method 1: Fuzzing of DQS Processes

Fuzzing is an effective method for assessing processes where there is either very little information or an overwhelming amount of information regarding how the process deals with the input streams being manipulated. After some time was spent developing a basic fuzzer for processes within the Siemens TG system that handle DQS messaging, it was determined that neither situation was applicable.

Part of the process of developing an effective fuzzer involves reversing or decoding the structure of the protocol being fuzzed. The more that is known about a protocol, the more specific test cases can be developed. Constraints in the protocol can be identified, which would otherwise prevent test cases fully exercising the target code base (i.e., integrity hashes or cyclic redundancy checks). In general, the more that is known about a protocol the more effective the fuzzer will be.

In practice, typically a basic "dumb" fuzzer[13] is quickly developed and then run with a number of test cases. While the "dumb" fuzzer runs, a "smart" fuzzer that takes into account protocol complexities is developed. In this assessment, investigating the DQS protocol and the processes that consume DQS messages lead to the determination that development of a "smart" fuzzer would not be prudent given the

11. Open SSL Ref: http://openssl.org.
12. Fuzzing: Fuzz testing or fuzzing is a black box software testing technique, which basically consists in finding implementation bugs using malformed/semi-malformed data injection in an automated fashion. Ref: The Open Web Application Security Project at http://www.owasp.org/index.php/Fuzzing.
13. A "dumb" fuzzer generates malformed data without concern for protocol structure or other requirements – while they can identify vulnerabilities, they are typically stopped by checksums and other protocol logic that frequently gets applied to network data packets before further processing occurs.

amount of time allocated for the task. The complexity in the TG system with regards to DQS processing is in the sheer number of processes that handle DQS messages, not in their individual complexity. It was more time efficient to simply evaluate the source code of an individual process to assess how it handled external inputs than it would have been to develop a fuzzer for each individual process. This due in part to the DQS protocol being used as a lower layer transport mechanism among processes, meaning that each individual process implemented its own message structure and protocol on top of DQS.

Still, a low-level "dumb" fuzzer was developed and run for the protocol layers that allow for transport of DQS messages over the network.

5.3.5.2 Vulnerability: ics_rbufstore_px Heap-based Buffer Overflow

There is a heap-based buffer overflow from attacker-controlled data into a dynamically allocated buffer in the *pllib* shared library residing on the Primary Host server (*inlhosta*).

This vulnerability potentially exists in any networked application that includes and uses the *pllib* shared library, and is not limited to the *wslan_server* process.

5.3.5.2.1 CVSS Base Metrics

Access Complexity (AC)

An attacker must at least bypass a hostname/IP check performed by the forwarding DQS process, and possibly bypass or complete an SSL negotiation before they can execute an attack targeting this vulnerability, depending on whether or not an optional security package has been installed.

The CVSS Access Complexity rating is Medium (M); access conditions are somewhat specialized. CVSS Rating: AC:M

Authentication (Au)

If the optional security package is installed, a single authentication step via SSL certificate is required. However, the default (without optional components) installation of the Power TG system does not require authentication.

The CVSS Authentication rating is None (N); authentication is not required to access and exploit the vulnerability. CVSS Rating: Au:N

Confidentiality Impact (C)

The CVSS Confidentiality Impact rating is Complete (C); there is a total information disclosure, resulting in all system files being revealed. Rating C:C

The attacker is able to read all of the system's data (memory, files, etc.).

Integrity Impact (I)

The CVSS Integrity Impact rating is Complete (C); there is a total compromise of system integrity. CVSS Rating: I:C

There is a complete loss of system protection, resulting in the entire system being compromised. The attacker is able to modify any files on the target system.

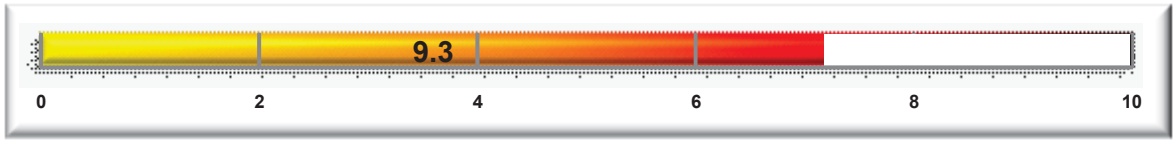
Availability Impact (A)

The CVSS Availability Impact rating is Complete (C); there is a total shutdown of the affected resource. CVSS Rating: A:C

The attacker can render the resource completely unavailable.

Vulnerability CVSS Score

Table 27. *ics_rbufstore_px* heap-based buffer overflow CVSS score.

Scoring Date:	**N/A**	 **CVSS Calculator**
Base Score	**9.3**	
Impact Subscore	10	
Exploitability Subscore	8.6	
Temporal Score	**Not Defined**	
Overall Score	**9.3**	
		
Vector	(AV:N/AC:M/Au:N/C:C/I:C/A:C)	

5.3.5.2.1 Mitigations

The primary and most effective mitigation for this vulnerability is to validate external inputs before they are used for memory allocation and for copying operations. This should be done for each variable that is assigned from a source external to the code or module that is using the variable. Libraries should be especially untrusting, as typically all of their inputs are going to be from external sources. This practice not only helps secure against attacks, but also helps reveal bugs in the application.

5.3.5.3 Method Conclusions

Due to the nature of the Siemens TG system discussed in Section 5.3.5.1 above, the amount of fuzzing performed was extremely limited. However, this method did uncover a fairly significant vulnerability with a CVSS overall score of 9.3 (out of 10), where an attacker has an unusual amount of control with regards to the environment they would be exploiting. The vulnerability showed an all too common case of library code trusting input parameters provided by an external source. Fortunately, this type of bug is well known, and simple verification of external parameters would immediately render the vulnerability non-existent.

If additional fuzzing were to be done, it would be done against the multitude of DQS message consumers, requiring a good amount of effort and customization. Additional time would need to be allocated to account for this effort.

5.3.5.4 Method 2: Source Code Review of DQS Processes

The method of source code review is primarily one of identifying code within a process that handles or interacts with user-supplied data. From there it is a matter of working through how that data is used by the process, and what a user (or attacker) can do to influence or corrupt the processes.

In many cases, source code review can be detrimental to the overall goal of identifying vulnerabilities, as the amount of time it takes to become familiar with the development environment and conventions used by developers may be prohibitive.

With the Siemens TG system, the source code provided as a standard part of the Linux installation proved to be clear enough to allow for relatively quick understanding.

The DQS protocol allows a process to send and receive messages in an orderly manner from other processes in the TG system. Routing of DQS messages is determined by a number of parameters, including Central Processing Units (CPUs) and process IDs. There are a few processes that provide a network "entry point" from which a networked application can insert a DQS message into the system, which will then be forwarded on to the appropriate process or system according to the CPU and process ID. There are a large number of processes that consume data from the DQS system, not all of which were looked at due to time constraints.

In each of the vulnerability tests illustrated below, the *wslan_server* process on *inlhosta* was used as the network entry point into the DQS system. The *wslan_server* process typically accepts DQS messages from workstation client machines within the TG system.

5.3.5.5 Vulnerability: FSP Process Invalid lanh_sendid Invalid Index/DoS

The FSP process uses an attacker-controlled value to index into an array, allowing for an invalid memory access, which will crash the process. This occurs during the processing of a "file copy request" packet sent to the FSP process via a DQS message.

The FSP process is marked as being "critical" in the *ProcessList.xml* configuration file for the Siemens TG system. Because of this, when the FSP process crashes, the entire set of applications on the host the process was running on are brought down as well, requiring a manual restart.

5.3.5.5.1 CVSS Base Metrics

Access Vector (AV)

The Access Vector metric ultimately depends on how the system is configured. Specifically, it depends on whether the host is setup to perform DNS queries for client hostnames, or if it is set up to perform local host file resolution. In the case of a local host file configuration, Adjacent Network access is required by an attacker to successfully exploit this vulnerability. In the DNS resolution configuration, only Network access is required.

The worst-case scenario is a DNS name resolution configuration that allows an attacker to spoof or manipulate a DNS response (or perform DNS Cache poisoning) from a remote network, providing them the opportunity to run an attack from an external network.

The CVSS Access Vector rating is Network (N)—A vulnerability exploitable with network access means the vulnerable software is bound to the network stack, and the attacker does not require local network access or local access. Such a vulnerability is often termed "remotely exploitable." CVSS Rating: AV:N

Access Complexity (AC)

An attacker must at least bypass a hostname/IP check performed by the forwarding DQS process, and possibly bypass or complete an SSL negotiation before they can execute an attack targeting this vulnerability, depending on whether or not an optional security package has been installed.

The CVSS Access Complexity rating is Medium (M); access conditions are somewhat specialized. CVSS Rating: AC:M

Authentication (Au)

If the optional security package is installed, a single authentication step via SSL certificate is required. However, the default (without optional components) installation of the Power TG system does not require authentication.

The CVSS Authentication rating is None (N); authentication is not required to access and exploit the vulnerability. CVSS Rating: Au:N

Confidentiality Impact (C)

The CVSS Confidentiality Impact rating is None (N); there is no impact to the confidentiality of the system. CVSS Rating: C:N

Integrity Impact (I)

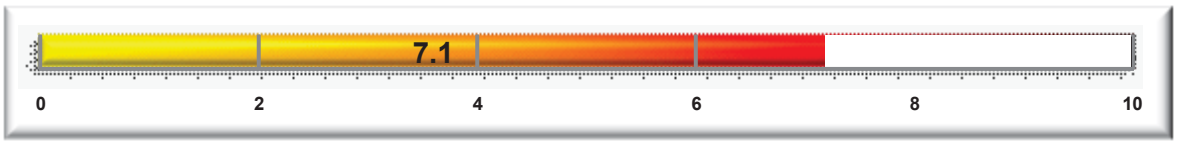
The CVSS Integrity Impact rating is None (N); there is no impact to the integrity of the system. CVSS Rating: I:N

Availability Impact (A)

The CVSS Availability Impact rating is Complete (C); there is a total shutdown of the affected resource. CVSS Rating: A:C

Vulnerability CVSS Score

Table 28. *FSP* process invalid *lanh_sendid* invalid index/DoS CVSS score.

Scoring Date:	**N/A**	 CVSS Calculator
Base Score	**7.1**	
Impact Subscore	6.9	
Exploitability Subscore	8.6	
Temporal Score	**Not Defined**	
Overall Score	**7.1**	
		
Vector	(AV:N/AC:M/Au:N/C:N/I:N/A:C)	

5.3.5.5.1 Mitigations

The most effective and recommended mitigation for this vulnerability is to validate externally supplied data before use. The validation would ensure that the data being supplied by an external party matches the expectations and operating requirements of the code that uses the outside data.

In the absence of data verification, a work around mitigation would be to ensure that no untrusted parties are able to send data to the vulnerable processes. For the Siemens TG system, this primarily means ensuring that there are absolutely no untrusted computers on the TG network, or any other network that the TG system interacts with.

5.3.5.6 Vulnerability: FSP Process FILE_DESCR_U Buffer Overflow/DoS

The FSP process uses an attacker-controlled value to delimit a for-loop, copying data from an attacker-controlled location into a statically allocated buffer. This occurs during the processing of a "file copy request" packet sent to the FSP process via a DQS message.

The FSP process is marked as being "critical" in the *ProcessList.xml* configuration file for the Siemens TG system. Because of this, when the FSP process crashes, the entire set of applications on the host the process was running on are brought down as well, requiring a manual restart.

5.3.5.6.1 CVSS Base Metrics

Access Vector (AV)

The Access Vector metric ultimately depends on how the system is configured. Specifically, it depends on whether the host is setup to perform DNS queries for client hostnames, or if it is set up to

perform local host file resolution. In the case of a local host file configuration, Adjacent Network access is required by an attacker to successfully exploit this vulnerability. In the DNS resolution configuration, only Network access is required.

The worst-case scenario is a DNS name resolution configuration that allows an attacker to spoof or manipulate a DNS response (or perform DNS Cache poisoning) from a remote network, providing them the opportunity to run an attack from an external network.

The CVSS Access Vector rating is Network (N)—A vulnerability exploitable with network access means the vulnerable software is bound to the network stack, and the attacker does not require local network access or local access. Such a vulnerability is often termed "remotely exploitable." CVSS Rating: AV:N

Access Complexity (AC)

An attacker must at least bypass a hostname/IP check performed by the forwarding DQS process, and possibly bypass or complete an SSL negotiation before they can execute an attack targeting this vulnerability, depending on whether or not an optional security package has been installed.

The CVSS Access Complexity rating is Medium (M); access conditions are somewhat specialized. CVSS Rating: AC:M

Authentication (Au)

If the optional security package is installed, a single authentication step via SSL certificate is required. However, the default (without optional components) installation of the Power TG system does not require authentication.

The CVSS Authentication rating is None (N); authentication is not required to access and exploit the vulnerability. CVSS Rating: Au:N

Confidentiality Impact (C)

The CVSS Confidentiality Impact rating is None (N); there is no impact to the confidentiality of the system. CVSS Rating: C:N

Integrity Impact (I)

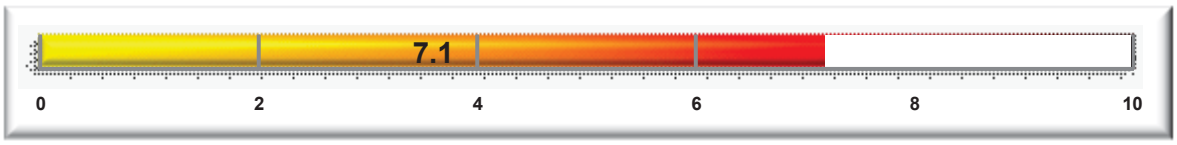
The CVSS Integrity Impact rating is None (N); there is no impact to the integrity of the system. CVSS Rating: I:N

Availability Impact (A)

The CVSS Availability Impact rating is Complete (C); there is a total shutdown of the affected resource. CVSS Rating: A:C

Vulnerability CVSS Score

Table 29. *FSP* process *FILE_DESCR_U* buffer overflow/DoS CVSS score.

Scoring Date:	**N/A**	 **CVSS Calculator**
Base Score	**7.1**	
Impact Subscore	6.9	
Exploitability Subscore	8.6	
Temporal Score	**Not Defined**	
Overall Score	**7.1**	
		
Vector	(AV:N/AC:M/Au:N/C:N/I:N/A:C)	

5.3.5.6.2 Mitigations

The most effective and recommended mitigation for this vulnerability is to validate externally supplied data before use. The validation would ensure that the data being supplied by an external party matches the expectations and operating requirements of the code that uses the outside data.

In the absence of data verification, a work around mitigation would be to ensure that no untrusted parties are able to send data to the vulnerable processes. For the Siemens TG system, this primarily means ensuring that there are absolutely no untrusted computers on the TG network, or any other network that the TG system interacts with.

Technically, a mitigation is already in place: the use of the "-check bounds" option in the Intel Fortran compiler build scripts. If it were not for this option, this vulnerability would result in arbitrary code execution instead of just a DoS condition. This mitigation is effective, but does not prevent an attacker from crashing the FSP process, or from bringing down the rest of the processes on the system.

5.3.5.7 Vulnerability: api_server Process process_appl_nbr() Stack-based Buffer Overflow

There is a stack-based buffer overflow from attacker-controlled data into a statically allocated buffer in the *api_server* process residing on the Primary Host server (*inlhosta*).

5.3.5.7.1 CVSS Base Metrics

Access Vector (AV)

The Access Vector metric ultimately depends on how the system is configured. Specifically, it depends on whether the host is setup to perform DNS queries for client hostnames, or if it is set up to perform local host file resolution. In the case of a local host file configuration, Adjacent Network access is required by an attacker to successfully exploit this vulnerability. In the DNS resolution configuration, only Network access is required.

The worst-case scenario is a DNS name resolution configuration that allows an attacker to spoof or manipulate a DNS response (or perform DNS Cache poisoning) from a remote network, providing them the opportunity to run an attack from an external network.

The CVSS Access Vector rating is Network (N)—A vulnerability exploitable with network access means the vulnerable software is bound to the network stack, and the attacker does not require local network access or local access. Such a vulnerability is often termed "remotely exploitable." CVSS Rating: AV:N

Access Complexity (AC)

An attacker must at least bypass a hostname/IP check performed by the forwarding DQS process, and possibly bypass or complete an SSL negotiation before they can execute an attack targeting this vulnerability, depending on whether or not an optional security package has been installed.

The CVSS Access Complexity rating is Medium (M); access conditions are somewhat specialized. CVSS Rating: AC:M

Authentication (Au)

If the optional security package is installed, a single authentication step via SSL certificate is required. However, the default (without optional components) installation of the Power TG system does not require authentication.

The CVSS Authentication rating is None (N); authentication is not required to access and exploit the vulnerability. CVSS Rating: Au:N

Confidentiality Impact (C)

The CVSS Confidentiality Impact rating is Complete (C); there is a total information disclosure, resulting in all system files being revealed. Rating C:C

The attacker is able to read all of the system's data (memory, files, etc.).

Integrity Impact (I)

The CVSS Integrity Impact rating is Complete (C); there is a total compromise of system integrity. CVSS Rating: I:C

There is a complete loss of system protection, resulting in the entire system being compromised. The attacker is able to modify any files on the target system.

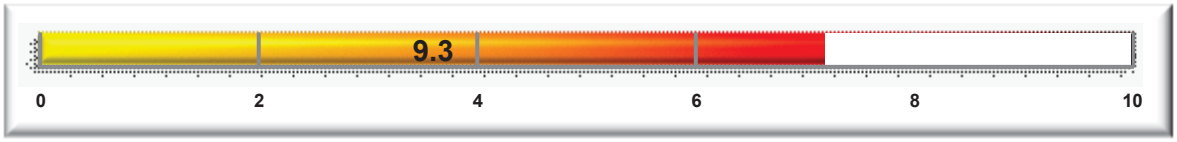
Availability Impact (A)

The CVSS Availability Impact rating is Complete (C); there is a total shutdown of the affected resource. CVSS Rating: A:C

The attacker can render the resource completely unavailable.

Vulnerability CVSS Score

Table 30. *api_server* Process *process_appl_nbr()* stack-based buffer overflow CVSS score.

Scoring Date:	**N/A**	 **CVSS Calculator**
Base Score	**9.3**	
Impact Subscore	10	
Exploitability Subscore	8.6	
Temporal Score	**Not Defined**	
Overall Score	**9.3**	
		
Vector	(AV:N/AC:M/Au:N/C:C/I:C/A:C)	

5.3.5.7.1 Mitigations

The primary and most effective mitigation would be to replace the input delimited *strcpy()* function with a explicitly delimited *strncpy()* call, where the maximum number of bytes copied from the input string to the destination buffer is explicitly passed as an argument to the function. Proper use of *strncpy()* function has been noted elsewhere in the Siemens TG codebase.

5.3.5.8 Vulnerability: api_server Process process_alarms_list() DoS

There is an attacker-delimited for-loop in the *api_server* process from the *process_alarms_list()* function that can result in a invalid memory access causing the application to terminate.

A test case was not developed for this vulnerability as it follows almost the exact code path as the vulnerability discussed in Section 5.3.5.6.25.3.5.6 which demonstrated sufficient feasibility of attack.

5.3.5.8.1 CVSS Base Metrics

Access Vector (AV)

The Access Vector metric ultimately depends on how the system is configured. Specifically, it depends on whether the host is setup to perform DNS queries for client hostnames, or if it is set up to perform local host file resolution. In the case of a local host file configuration, Adjacent Network access is required by an attacker to successfully exploit this vulnerability. In the DNS resolution configuration, only Network access is required.

The worst-case scenario is a DNS name resolution configuration that allows an attacker to spoof or manipulate a DNS response (or perform DNS Cache poisoning) from a remote network, providing them the opportunity to run an attack from an external network.

The CVSS Access Vector rating is Network (N)—A vulnerability exploitable with network access means the vulnerable software is bound to the network stack, and the attacker does not require local network access or local access. Such a vulnerability is often termed "remotely exploitable." CVSS Rating: AV:N

Access Complexity (AC)

An attacker must at least bypass a hostname/IP check performed by the forwarding DQS process, and possibly bypass or complete an SSL negotiation before they can execute an attack targeting this vulnerability, depending on whether or not an optional security package has been installed.

The CVSS Access Complexity rating is Medium (M); access conditions are somewhat specialized. CVSS Rating: AC:M

Authentication (Au)

If the optional security package is installed, a single authentication step via SSL certificate is required. However, the default (without optional components) installation of the Power TG system does not require authentication.

The CVSS Authentication rating is None (N); authentication is not required to access and exploit the vulnerability. CVSS Rating: Au:N

Confidentiality Impact (C)

The CVSS Confidentiality Impact rating is None (N); there is no impact to the confidentiality of the system. CVSS Rating: C:N

Integrity Impact (I)

The CVSS Integrity Impact rating is None (N); there is no impact to the integrity of the system. CVSS Rating: I:N

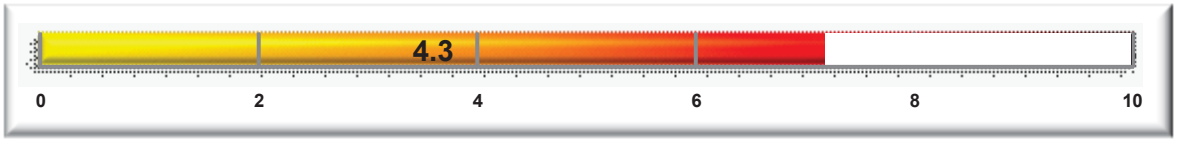
Availability Impact (A)

The CVSS Availability Impact rating is Partial (P); there is reduced performance or interruptions in resource availability. CVSS Rating: A:P

A successful DoS attack would bring down the *api_server* process, which would require a manual restart. The rest of the processes on the host would be unaffected. This rating would have been Complete if the *api_server* process was marked as critical, which would have caused the entire system to shutdown when the process was crashed.

Vulnerability CVSS Score

Table 31. *api_server* process *process_alarms_list()* DoS CVSS score.

Scoring Date:	**N/A**	 **CVSS Calculator**
Base Score	**4.3**	
Impact Subscore	2.9	
Exploitability Subscore	8.6	
Temporal Score	**Not Defined**	
Overall Score	**4.3**	
		
Vector	(AV:N/AC:M/Au:N/C:N/I:N/A:P)	

5.3.5.8.1 Mitigations

The primary and only real effective mitigation for this vulnerability would be to validate the input parameter before it is used as a delimiter in the for-loop. In this case, the program would need to ensure that the *num_chgd_entries* was not larger than the actual number of entries provided in the DQS message being processed.

5.3.5.9 Vulnerability: api_server Process apisrv_process_spo_tag() Stack-based Buffer Overflow

There is a stack-based buffer overflow from attacker-controlled data into a statically allocated buffer in the *api_server* process residing on the Primary Host server (*inlhosta*).

A test case was not developed for this vulnerability as it follows almost the exact code path as the vulnerability discussed in Section 5.3.5.6, which demonstrated sufficient feasibility of attack.

5.3.5.9.1 CVSS Base Metrics

Access Vector (AV)

The Access Vector metric ultimately depends on how the system is configured. Specifically it depends on whether the host is setup to perform DNS queries for client hostnames, or if it is set up to perform local host file resolution. In the case of a local host file configuration, Adjacent Network access

is required by an attacker to successfully exploit this vulnerability. In the DNS resolution configuration, only network access is required.

The worst-case scenario is a DNS name resolution configuration that allows an attacker to spoof or manipulate a DNS response (or perform DNS Cache poisoning) from a remote network, providing them the opportunity to run an attack from an external network.

The CVSS Access Vector rating is Network (N)—A vulnerability exploitable with network access means the vulnerable software is bound to the network stack, and the attacker does not require local network access or local access. Such a vulnerability is often termed "remotely exploitable." CVSS Rating: AV:N

Access Complexity (AC)

An attacker must at least bypass a hostname/IP check performed by the forwarding DQS process, and possibly bypass or complete an SSL negotiation before they can execute an attack targeting this vulnerability, depending on whether or not an optional security package has been installed.

The CVSS Access Complexity rating is Medium (M); access conditions are somewhat specialized. CVSS Rating: AC:M

Authentication (Au)

If the optional security package is installed, a single authentication step via SSL certificate is required. However, the default (without optional components) installation of the Power TG system does not require authentication.

The CVSS Authentication rating is None (N); authentication is not required to access and exploit the vulnerability. CVSS Rating: Au:N

Confidentiality Impact (C)

The CVSS Confidentiality Impact rating is Complete (C); there is a total information disclosure, resulting in all system files being revealed. Rating C:C

The attacker is able to read all of the system's data (memory, files, etc.).

Integrity Impact (I)

The CVSS Integrity Impact rating is Complete (C); there is a total compromise of system integrity. CVSS Rating: I:C

There is a complete loss of system protection, resulting in the entire system being compromised. The attacker is able to modify any files on the target system.

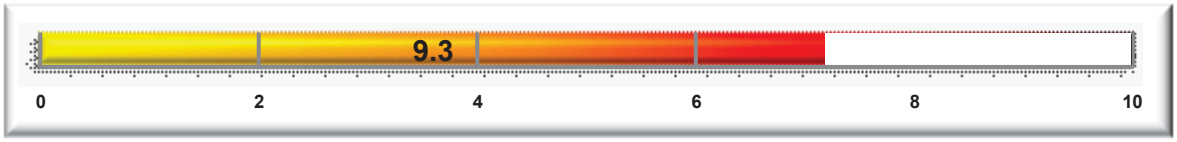
Availability Impact (A)

The CVSS Availability Impact rating is Complete (C); there is a total shutdown of the affected resource. CVSS Rating: A:C

The attacker can render the resource completely unavailable.

Vulnerability CVSS Score

Table 32. *api_server* process *apisrv_process_spo_tag()* stack-based buffer overflow CVSS score.

Scoring Date:	**N/A**	 **CVSS Calculator**
Base Score	**9.3**	
Impact Subscore	10	
Exploitability Subscore	8.6	
Temporal Score	**Not Defined**	
Overall Score	**9.3**	
		
Vector	(AV:N/AC:M/Au:N/C:C/I:C/A:C)	

5.3.5.9.1 Mitigations

The primary and most effective mitigation would be to replace the input delimited *strcpy()* function with a explicitly delimited *strncpy()* call, where the maximum number of bytes copied from the input string to the destination buffer is explicitly passed as an argument to the function. Proper use of *strncpy()* function has been noted elsewhere in the Siemens TG codebase.

5.3.5.10 Method Conclusions

The vulnerabilities identified by this method follow the basic trend of unsecure coding practices. A primary tenant of secure coding is to not trust external inputs. Each of the five vulnerabilities identified by this method is the result of not validating external inputs before use. In each case, validation of the external inputs would successfully mitigate the vulnerability.

In some situations, external input validation is not possible. In these cases, the developer should rely on functions that allow them to be explicit in specifying the desired outcome of the function. For example, using *strncpy()* instead of *strcpy()* allows the developer to explicitly define the maximum number of bytes that should be copied from the source string buffer to the destination string buffer. In fact, the *strcpy()* function, along with a growing list of other functions in the standard C library, are so frequently used insecurely that they are banned from use by developers in major software development companies such as Microsoft. Performing a quick non-validated search through the source provided in the Power TG system reveals almost 6,000 uses of the *strcpy()* function. It is certain (based upon what the researchers have seen in this assessment) that a vast majority of those *strcpy()* calls are not exploitable; however, even if just 1% of them were, there would be approximately 60 exploitable vulnerabilities.

The Siemens Power TG system has been in development for a long time, with sections of the system having been developed before the advent of secure coding practices. Different processes that had been written at different periods in the system development show an obvious difference in how they treat external inputs, and how they handle error conditions. The later development shows instances of secure coding practices, where the earlier development shows a complete lack of concern. It is strongly recommended that the older code base be refactored (or in some cases, completely rewritten) with a security mindset.

The CVSS overall scores for the vulnerabilities range from 9.3 to 4.3 (out of 10) depending on whether or not the vulnerability was a DoS or arbitrary code execution, and upon whether or not the process was marked as critical within the Power TG system resulting in a single process DoS or an entire system DoS.

This method also identified a number of other vulnerabilities that are detailed in the AT2 cyber report, as they do not directly pertain to the DQS protocol.

5.3.5.11 Method 3: Reverse Engineering of Optional Security Package

The optional security package for the Siemens Power TG system aims to prevent unauthenticated communication with any of the services it provides over the network. Without the security package, the system—by design—allows for networked hosts to issue commands to the system, limited only by a hostname check performed either locally or via DNS requests. The ability of an attacker to bypass the simple hostname checks was demonstrated in the Phase 1 assessment performed by INL.

In an effort to evaluate the ability of an attacker to inject DQS messages into a system protected by the optional security package, the security package itself was investigated. Source code was not available for the security library, and so the shared library that the security package consists of was reverse engineered, looking for ways an attacker may either attack the library itself or bypass its protections.

The security package is built around the open source library OpenSSL. The use of a mature and existing cryptography library is commended as developing cryptography applications is notoriously difficult and error prone. Even so, configuration errors and misuse of the OpenSSL library can also lead to security issues.

5.3.5.12 Vulnerability: ProjectCA Certificate Not Validated in Certificate Chain

The Power TG security package does not validate that the Project Certificate Authority (ProjectCA) certificate provided by a potential client matches the ProjectCA certificate used by the particular installation involved. This allows anyone who has a signed ProjectCA certificate to create "valid" certificates for any other Power TG system, which in certain circumstances allows them to bypass the security package entirely.

5.3.5.12.1 CVSS Base Metrics

Access Vector (AV)

The Access Vector metric ultimately depends on how the system is configured. Specifically, it depends on whether the host is setup to perform DNS queries for client hostnames, or if it is set up to perform local host file resolution. In the case of a local host file configuration, Adjacent Network access is required by an attacker to successfully exploit this vulnerability. In the DNS resolution configuration, only network access is required.

The worst-case scenario is a DNS name resolution configuration that allows an attacker to spoof or manipulate a DNS response (or perform DNS Cache poisoning) from a remote network, providing them the opportunity to run an attack from an external network.

The CVSS Access Vector rating is Network (N)—A vulnerability exploitable with network access means the vulnerable software is bound to the network stack, and the attacker does not require local

network access or local access. Such a vulnerability is often termed “remotely exploitable.” CVSS Rating: AV:N

Access Complexity (AC)

The attacker must identify a hostname of the client they are going to create a fake certificate for, as well as understand the communication relationship requirements set forth by the system configuration (i.e., not every host within the Power TG system is permitted to access every service). The difficulty in meeting these prerequisites can range from simple to marginally complex, depending on the installation.

The CVSS Access Complexity rating is Medium (M); access conditions are somewhat specialized. CVSS Rating: AC:M

Authentication (Au)

This is a vulnerability in the authentication of hosts, allowing an attacker to bypass normal authentication methods based upon SSL certificates.

The CVSS Authentication rating is None (N); authentication is not required to access and exploit the vulnerability. CVSS Rating: Au:N

Confidentiality Impact (C)

The CVSS Confidentiality Impact rating is Complete (C); there is a total information disclosure, resulting in all system files being revealed. Rating C:C

Integrity Impact (I)

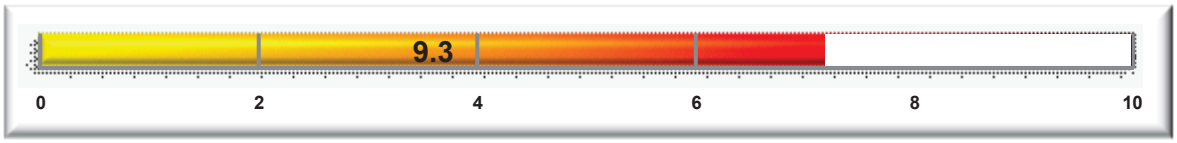
The CVSS Integrity Impact rating is Complete (C); there is a total compromise of system integrity. CVSS Rating: I:C

Availability Impact (A)

The CVSS Availability Impact rating is Complete (C); there is a total shutdown of the affected resource. CVSS Rating: A:C

Vulnerability CVSS Score

Table 33. ProjectCA certificate not validated in certificate chain CVSS score.

Scoring Date:	**N/A**	
Base Score	**9.3**	
Impact Subscore	10	
Exploitability Subscore	8.6	
Temporal Score	**Not Defined**	**CVSS Calculator**
Overall Score	**9.3**	
		
Vector	(AV:N/AC:M/Au:N/C:C/I:C/A:C)	

5.3.5.12.1 Mitigations

The most effective and only real mitigation would be for Siemens Power TG to rewrite their certificate verification method to verify that the ProjectCA certificate provided by a client matches the ProjectCA certificate of the distinct Power TG installation.

In the absence of a patched certificate verification method, users may increase the complexity of attack by not using DNS within their Power TG system, as that forces an attacker to be on an adjacent network, allowing them to spoof an IP address of a client. It would also be beneficial to follow a policy of least privileged access by limiting network access to any Power TG host from any system not absolutely required to have access.

5.3.5.13 Method Conclusions

The vulnerability identified via this method is rather significant (it has a CVSS overall score of 9.3). It is primarily a vulnerability of trust as opposed to a technical vulnerability. Given this vulnerability, a user of the security package for TG goes from trusting Siemens TG and their own local administrator of their Project Certificate Authority to trusting every organization that has purchased or tested a Siemens TG system, regardless of how well they control access to their Project Certificate Authority.

Apart from this vulnerability, and the outdated version of OpenSSL used on the Linux hosts, the implementation of the security package appears to have been done well. It provides a necessary layer of authentication and message integrity that would otherwise be sorely lacking in the Siemens TG system, and should be part of a standard installation instead of an optional add-on component. As with other security technologies, defaulting to a secure state of the system is better than defaulting to an unsecure state, from both marketing and security standpoints.

5.3.6 Conclusions

All of the vulnerabilities identified, with the exception of the ProjectCA certificate vulnerability, are a result of unsecure coding practices, namely not validating external inputs/data before use. The ProjectCA certificate vulnerability is a result of how the validation algorithm checks certificates provided

by potential clients and servers. The ProjectCA certificate vulnerability is the most significant, allowing any owner of a signed ProjectCA certificate signed by the PowerTG Root certificate to establish an authenticated connection to any Power TG host, regardless of whether or not they have a valid host certificate for any particular system. It allows for the effective bypass of the entire optional security package.

The remaining vulnerabilities range in significance, based upon a number of mitigating factors. One mitigating factor that applies to all of the vulnerabilities is the DNS hostname/IP check each service performs on a supplicating client before allowing a connection. This mitigation is relatively simple for an attacker to bypass, depending on their location on the target network. The use of a static hostname file on each host as opposed to DNS resolution is recommended as the more secure configuration for the Power TG system. It is not foolproof, but requires an attacker to be on an adjacent network as defined by the CVSS system as opposed to a remote network, as the DNS configuration would allow.

In spite of the ProjectCA certificate vulnerability, the optional security package is by far the most secure deployment, and is recommended for all installations—so much so that it should be a standard (and not optional) part of the Power TG system, as it provides a minimum acceptable level of secure authentication for the entire system. Without the optional security package, any host with the Power TG system software installed would be wide open for abuse by a knowledgeable attacker. The services necessary for the Power TG system to operate are extremely trusting of external input and commands—by design. Without the security package, anyone with network access will be able to issue commands to the system.

It is strongly recommended that a secure code review be performed on the source tree, with initial attention paid to the use of unsafe functions such as *strcpy()*. Removing the unsecure functions and replacing them with their equivalent explicitly controlled versions would go a long way in security-per-dollar improvement.

Further assessments, if performed, should continue to focus on processes that consume DQS messages like the *api_server* and *FSP* processes.

5.4 Target 4 – Source Database (SDB)

5.4.1 Introduction

The objective of this target is to assess the SDB host from the Siemens Power TG system. Specifically, INL researchers looked for ways to manipulate the configuration and security information that the SDB provides to other hosts and servers from an unprivileged or unauthenticated position.

This section attempts to extract the pertinent information from the Cyber Researcher's report on AT4. The Cyber Researcher's report documents to a level where "someone similarly skilled in the art" can reproduce the results. This level is not required for the general report. For the reader that needs this level of detail, read the attached Cyber Researcher's report: Siemens Spectrum Power TG Cyber Report for AT4 – Source Database (SDB).

Siemens Spectrum
Power TG Cyber Repo

5.4.2 Significance

The SDB is an important target because of its role in the configuration of almost every machine within the Power TG system. Success of an attack modifying the SDB database could negatively impact the operation of the overall system.

5.4.3 Assessment

Areas assessed during this target include the SDB server (*INLSDB*) on the INL Test Power TG system, the communication path between the *INLSDB* server and remote SDB client, source code for stored procedures, the *tg_configserver* and *tg_rshserver* processes on the *INLSDB* server, and the SDB client itself. The *INLSDB* server was assessed for configuration errors, unnecessary open ports, and blank or default passwords. The communication path between the server and client was analyzed for clear text authentication and message passing. Stored procedures associated with interesting functions of the SDB client were reviewed for programming vulnerabilities. The *tg_rshserver* and *tg_configserver* underwent basic reverse engineering and debugging to try to identify programming vulnerabilities. The SDB client was tested for SQL injection and related input validation problems.

5.4.3.1 Method 1: Network Analysis

The focus of this method is to identify concerns and vulnerabilities related to protocols, ports, and services on the network. A scanning tool such as Nmap was used to identify open ports on networked systems. Analysis tools like TCPView or Process Explorer were used to identify the owning process for each open port. Wireshark[14] was used to identify and analyze the protocols and connections between the SDB server and client.

5.4.3.2 Concern: Clear Text Messages

This method used Wireshark to capture, analyze, and dissect the communications between the SDB Client, located on the stand alone workstation (*SDB*), and the main Microsoft SQL database (on *INLSDB*). The goals for this method are to obtain database credentials passed in clear text and to gather information about the structure and methods used for accessing the data stored in the database. Fortunately, all authentication packets appear to be using a form of encryption to pass database credentials. However, once authentication completed all database queries and responses are passed in clear text.

Given time, an attacker could obtain enough information to identify key tables, stored procedures, data, and the basic structure of the database. The current Siemens Power TG test system does not appear to be using any form of encryption beyond what is used for authentication. As a result, it is possible for an attacker to insert arbitrary values into the SQL queries passed in the clear. A proof-of-concept was attempted to illustrate this point, but due to time constraints and unforeseen software bugs, it was not successful. The recommended mitigation for this concern is to configure Microsoft SQL Server 2008 to force encryption for network connections. This would prevent an attacker from seeing or manipulating SQL queries or responses passed between the client and server.

Testing of the SDB client with forced encryption did not appear to have any impact on the responsiveness and usability of the client.

5.4.3.3 Port Analysis

In addition to the network traffic analysis, a port analysis was performed to try to identify unnecessary open ports on the *INLSDB* server. Fortunately, the results of the Nmap scans of the *INLSDB* server showed no unnecessary open ports.

14. Wireshark Ref: http://www.wireshark.org/.

Reverse engineering and debugging efforts of this target found no immediate concerns or vulnerabilities for the owning processes. However, some issues were identified in AT6 for the *tg_rshserver.exe* process.

5.4.3.4 Method Conclusions

Although no vulnerabilities were identified during Network Analysis, a couple of concerns were identified. The most significant being the use of clear text messages to pass information after authentication. This enables an attacker to obtain valuable information about the database structure as well as the data being passed in the clear. An attacker would also be able to insert arbitrary values into the SQL queries passed in the clear. If the attacker obtains control of the communication channel, it would cause serious impacts to the confidentiality, integrity, and availability of the database. The recommended mitigation is to force encryption on the SQL Server 2008 side, which forces all that connect to use encryption.

5.4.3.5 Method 2: Input Validation Testing & Source Code Review

The focus of this method was to identify SQL vulnerabilities in the SDB client that could provide an attacker the ability to manipulate the data stored in the main SQL database.

5.4.3.6 Vulnerability: Data Routing Definition Form SQL Injection Zero Day Vulnerability

A SQL injection was identified in the Data Routing Form, under the Data Routing Definition tab, and the Source Station field.

5.4.3.6.1 CVSS Base Metrics

Access Vector (AV)

The vulnerability is accessed through the SDB client, which is a Microsoft Access front end, by entering invalid input into the Source Station field on the Data Routing Definition form. Access to the SDB client requires remote desktop or physical access to the stand alone workstation (SDB).

The CVSS Access Vector rating is Local (L)—A vulnerability exploitable with only *local access* requires the attacker to have either physical access to the vulnerable system or a local (shell) account. CVSS Rating: AV:L

Access Complexity (AC)

Exploitation of this vulnerability would be very difficult given the limited set of abilities that are offered by MS Access and the SQL injection. A deep knowledge and understanding of MS Access and its connectivity with SQL Server would be required to create an exploit for this vulnerability.

The CVSS Access Complexity rating is High (H); specialized access conditions exist. CVSS Rating: AC:H

Authentication (Au)

It is assumed that the attacker already has access to the physical machine or is able to access the machine remotely. Authentication against the SQL Server database is required by the attacker before access is granted to the SDB client interface where the SQL injection is located.

The CVSS Authentication rating is Single (S); one instance of authentication is required to access and exploit the vulnerability. CVSS Rating: Au:S

Confidentiality Impact (C)

Successful exploitation of this vulnerability would give the attacker the ability to access portions of the main SQL database that are cached locally on the system. Successful exploitation may also provide the attacker the ability to request additional information, from the main SQL Server database, that pertains to the locally cached data.

The CVSS Confidentiality Impact rating is Partial (P); there is considerable informational disclosure. Rating C:P

Integrity Impact (I)

Successful exploitation would partially impact the integrity of the data. The attacker would have access to the locally cached information of the main database. The following integrity impact rating is based solely on the data or files that could be modified by the attacker and does not consider the cascading effects that could result from the attacker's changes.

The CVSS Integrity Impact rating is Partial (P); modification of some system files or information is possible. CVSS Rating: I:P

Availability Impact (A)

Assuming the attacker has the ability to modify records locally it may be possible to partially impact the availability of the main SQL database when it is synchronized with the local cache. Changes to the database may not be realized immediately, but rather the next time a configuration is pushed out. The magnitude of the availability impact at the time of the push depends upon the change and the systems affected by the change. Regardless of the change, the operating system of the affected systems would continue to operate resulting in partial impact of availability.

The CVSS Availability Impact rating is Partial (P); there is reduced performance or interruptions in resource availability. CVSS Rating: A:P

Vulnerability CVSS Score

Table 34. SQL injection zero-day vulnerability CVSS score.

Scoring Date:	**N/A**	 **CVSS Calculator**
Base Score	**3.5**	
Impact Subscore	6.4	
Exploitability Subscore	1.5	
Temporal Score	**Not Defined**	
Overall Score	**3.5**	
		
Vector	(AV:L/AC:H/Au:S/C:P/I:P/A:P)	

5.4.3.6.1 Mitigations

The recommended mitigation for this vulnerability is two-fold. The first part is to perform better input validation. This SQL injection could be eliminated by checking for all possible special SQL characters—in this case the single and double quote characters, which were used to identify this vulnerability. Another approach for input validation is to whitelist all allowed characters, which may be easier than blacklisting special characters. Either way, care needs to be taken when dealing with user input. A good rule of thumb is to always handle user input as if it were malicious. The second part of the mitigation is to mask detailed database errors. By eliminating detailed feedback, it is more difficult for an attacker to identify that there is a problem with a particular input field.

5.4.3.7 Method Conclusions

This method identified a SQL injection vulnerability and some concerns regarding input validation checking. The SQL injection received an overall CVSS rating of 3.5. If this vulnerability was exploited it would directly affect the local MS Access caching database and indirectly affect the main SQL database on the *INLSDB* server. The main conclusion to be drawn from this method is that there is a failure to properly validate all user input. Evidence of this concern stems from the fact there other input fields that caused the SDB client to either crash or unnecessarily produce detailed SQL error messages. In either case, these behaviors are an indicator that not enough input validation testing and error handling is being done. Although attempts to exploit the SQL injection were unsuccessful, given enough time and research it may be possible to exploit.

5.4.3.8 Method 3: Reverse Engineering

Basic reverse engineering was done using IDA Pro disassembler[15] and OllyDbg on the *tg_rshserver*.exe and *tg_configserver.exe* processes, which reside on the *INLSDB* server. No vulnerabilities or major concerns were identified as part of the work performed on this Assessment Target. However, additional analysis of the *tg_rshserver*.exe binary was done in the work for AT6, where vulnerabilities were identified. The results from that work should be reviewed to determine the impacts to the *INLSDB* server and SQL database.

The *tg_configserver.exe* process provides a mechanism by which the SDB can transfer configuration files to each of the hosts within the Power TG system. Some of these files are sensitive in nature, specifically the private and public keys assigned to each individual host. If an attacker were able to bypass the OpenSSL-based authentication mechanism for this service, he/she would be able to easily acquire the private keys for other hosts in the system. An attacker would also be able to obtain the network configuration files for each host. One such bypass method is identified in Section 5.3. It is recommended that extra attention be paid to the authentication mechanism for this service as it can essentially provide unmitigated access to the system as a whole.

5.4.4 Conclusions

Overall, this assessment target was a partial success because no pure unauthenticated or unprivileged manipulation of the database could be achieved. However, a minor SQL injection and number of concerns were identified that could assist an attacker in achieving the goal of unauthenticated or unprivileged access to the main SQL database.

A single SQL injection vulnerability, with an overall CVSS rating of 3.5, was identified during this assessment target. This vulnerability stemmed primarily from a coding bug, but could have been prevented or reduced with better input validation and error handling. Although no other vulnerabilities were identified, there were several concerns that require attention. The first is the need for improved input validation. As mentioned in the body of this target, a number of problems were caused by not properly restricting or filtering the characters a user could use. All user input should be handled as if it is malicious. Better handling of error conditions should be done to prevent detailed messages from the server being displayed to the user. Finally, all network communications between the main SQL database should be fully encrypted to help prevent an attacker from obtaining or manipulating any information in the database. This should be a reasonable expectation as communications between the SDB client and server do not appear to be critically time sensitive. Any delays associated with encryption did not appear to noticeably impact the user's experience.

5.5 Target 5 – Web Server

5.5.1 Introduction

This assessment target will assess the functionality provided/used by the Siemens Power TG Web Server for exploitable vulnerabilities. Specifically, the work will focus on looking at various types of injections, look for opportunities to take control of the control system, and bypass restrictions imposed on the web server.

This section attempts to extract the pertinent information from the Cyber Researcher's report on AT5. The Cyber Researcher's report documents to a level where "someone similarly skilled in the art" can reproduce the results. This level is not required for the general report. For the reader

15. IDA Pro disassembler: Ref: http://www.hex-rays.com/idapro/.

that needs this level of detail, read the attached Cyber Researcher's report: Siemens Spectrum Power TG Cyber Report for AT5 – Web Server.

5.5.2 Significance

The web server can be configured in many different ways, with different access restrictions that can vary from allowing local subnet access to allowing access from remote networks. If the web server is allowed to be accessed by a different network, vulnerabilities in the web server software could allow an attacker a foothold into the Power TG system.

5.5.3 Rules of Engagement

The web server used for the assessment was configured to be a read-only HMI and had access controls in place so that a user had to authenticate to the web server to view web server resources. Certain parts of the assessment assumed that the attacker has access to the web interface as well as credentials to authenticate to the web server.

5.5.4 Assessment

The web server contains an interface to a control system HMI. The server runs Apache Web Server and Perl modules as the backend language. This assessment target focused on the web interface provided by the web server, assessing primarily the Apache deployment and Perl modules.

5.5.4.1 Method 1: Bypass Authentication/Security

Access to all the features hosted by the web server can be restricted to authenticated users only. Using Apache's basic authentication method, when a user tries to access content on the web server, the user must supply valid credentials to complete the request. The user credentials are then encoded and sent in clear text from the client to the web server. This authentication method requires credentials every time you access something from the web server, including web-style sheets, HTML files, images, and scripts. Modern web browsers will store and automatically send the encoded credentials along with each request to the server, making the authentication mostly transparent as it requires the user to provide credentials only once for each session.

5.5.4.2 Vulnerability: Unauthorized Access to Web Server HMI

The use of basic authentication in Apache allows unauthorized access to the web server HMI. Basic authentication is one of a number of different authentication methods available with the Apache web server. It is trivial to bypass, requiring the attacker to simply capture a single instance of the authentication tokens being passed from the client to the server. Since the authentication tokens are provided automatically by the web client for each request to the server (as discussed above), the chances are high that an attacker would be able to sniff the tokens assuming they had network access to the system.

5.5.4.2.1 CVSS Base Metrics

Access Vector (AV)

The CVSS Access Vector rating is Network (N)—A vulnerability exploitable with network access means the vulnerable software is bound to the network stack, and the attacker does not require local

network access or local access. Such a vulnerability is often termed “remotely exploitable.” CVSS Rating: AV:N

Access Complexity (AC)

The CVSS Access Complexity rating is Low (L); specialized access conditions or extenuating circumstances do not exist. CVSS Rating: AC:L

Authentication (Au)

The CVSS Authentication rating is None (N); authentication is not required to access and exploit the vulnerability. CVSS Rating: Au:N

Confidentiality Impact (C)

The CVSS Confidentiality Impact rating is Partial (P); there is considerable informational disclosure. Rating C:P

Integrity Impact (I)

The CVSS Integrity Impact rating is Partial (P); modification of some system files or information is possible. CVSS Rating: I:P

Availability Impact (A)

The CVSS Availability Impact rating is None (N); there is no impact to the availability of the system. CVSS Rating: A:N

Vulnerability CVSS Score

Table 35. Unauthorized access to web server HMI CVSS score.

Scoring Date:	**N/A**	 **CVSS Calculator**
Base Score	**6.4**	
Impact Subscore	4.9	
Exploitability Subscore	10	
Temporal Score	**Not Defined**	
Overall Score	**6.4**	
		
Vector	(AV:N/AC:L/Au:N/C:P/I:P/A:N)	

5.5.4.2.1 Mitigations

Referring to Apache’s security caveat, if basic authentication is to be used, it would be significantly more secure with an SSL connection. There are also other forms of authentication that can be used through Apache, including but not limited to digest authentication and database authentication.

5.5.4.3 Method Conclusions

Apache's basic authentication methodology is trivial to bypass. Apache has issued a security caveat that says not to use basic authentication for anything that requires real security. Apache offers other authentication methods that are more secure than basic authentication.

5.5.4.4 Method 2: Unused Files/Ports/Scripts

Unused files or scripts may give more information to an attacker or introduce additional flaws or vulnerabilities.

The web server backend uses mostly Perl scripts to create the Hypertext Markup Language (HTML) files accessed by web users. The Perl files used to create the functionality of the web server were next assessed for flaws, weaknesses, and injections.

5.5.4.4.1 Security Concern

When assessing a target, an attacker tries to gain as much information about the target as possible. Information that an attacker can gain with doing the smallest amount of work is always valuable for the attacker. A Perl script that provides a lot of information about the web server's system is available on the web server and accessible via a web browser.

5.5.4.5 Method 3: String Injections

A string injection is when user input is incorrectly filtered for string literal escape characters allowing attackers to inject code or commands to be executed by the system. User input is typically seen in web forms asking for typical things like user names, passwords, addresses, phone numbers, etc. For instance, if user input is not properly filtered, an attacker may be able to inject code or commands that are executed on the web server. User input can also be indirectly sent outside of forms by the user, such as within cookies and via parameters in GET and POST requests.

Although the Siemens TG web server system does not have any direct user input, it does accept indirect user input.

5.5.4.6 Vulnerability: String Injection Allows for Code Execution

There is a string injection vulnerability that could change the Uniform Resource Locator (URL), which could lead to code execution.

5.5.4.6.1 CVSS Base Metrics

Access Vector (AV)

The CVSS Access Vector rating is Network (N)—A vulnerability exploitable with network access means the vulnerable software is bound to the network stack, and the attacker does not require local network access or local access. Such a vulnerability is often termed "remotely exploitable." CVSS Rating: AV:N

Access Complexity (AC)

The CVSS Access Complexity rating is Low (L); specialized access conditions or extenuating circumstances do not exist. CVSS Rating: AC:L

Authentication (Au)

The CVSS Authentication rating is Single (S); one instance of authentication is required to access and exploit the vulnerability. CVSS Rating: Au:S

Confidentiality Impact (C)

The CVSS Confidentiality Impact rating is Complete (C); there is a total information disclosure, resulting in all system files being revealed. Rating C:C

Integrity Impact (I)

The CVSS Integrity Impact rating is Complete (C); there is a total compromise of system integrity. CVSS Rating: I:C

Availability Impact (A)

The CVSS Availability Impact rating is Complete (C); there is a total shutdown of the affected resource. CVSS Rating: A:C

A blacklist of characters could be created to search user input and filter out. A whitelist of characters may be a better option by only allowing certain characters.

Vulnerability CVSS Score

Table 36. String injection allows for code execution CVSS score.

Scoring Date:	**N/A**	 **CVSS Calculator**
Base Score	**9**	
Impact Subscore	10	
Exploitability Subscore	8	
Temporal Score	**Not Defined**	
Overall Score	**9**	
		
Vector	(AV:N/AC:L/Au:S/C:C/I:C/A:C)	

5.5.4.6.1 Mitigations

Mitigations to string injections are already well documented on the Internet and security books. Type filtering is done in the current Perl code, but there is no syntax filtering. Typically, user input is filtered for string literal escape characters, among others.

5.5.4.7 Method Conclusions

A string injection exists that allows an attacker to get remote code execution on the web server, *INLweb*. The injection executes arbitrary code as the *powertgweb* user who has administrator privileges. Mitigations are well known and documented on the Internet and security books. It is recommended that the Perl backend do syntax filtering via a blacklist or whitelist filter.

5.5.4.8 Method 4: Null Byte Injections

A null byte injection is when a null byte (%00 url encoded or 0x00 in hex) is injected into a user-supplied data field that typically results altering the logic of a web application.

5.5.4.9 Vulnerability: Null Byte Injection Bypasses Display Restrictions

There is a null byte injection vulnerability that would allow an authenticated user access to any display regardless of the settings in the *denied_disps* file.

5.5.4.9.1 CVSS Base Metrics

Access Vector (AV)

The CVSS Access Vector rating is Network (N)—A vulnerability exploitable with network access means the vulnerable software is bound to the network stack, and the attacker does not require local network access or local access. Such a vulnerability is often termed "remotely exploitable." CVSS Rating: AV:N

Access Complexity (AC)

The CVSS Access Complexity rating is Medium (M); access conditions are somewhat specialized. CVSS Rating: AC:M

Authentication (Au)

The CVSS Authentication rating is Single (S); one instance of authentication is required to access and exploit the vulnerability. CVSS Rating: Au:S

Confidentiality Impact (C)

The CVSS Confidentiality Impact rating is Partial (P); there is considerable informational disclosure. Rating C:P

Integrity Impact (I)

The CVSS Integrity Impact rating is None (N); there is no impact to the integrity of the system. CVSS Rating: I:N

Availability Impact (A)

The CVSS Availability Impact rating is None (N); there is no impact to the availability of the system. CVSS Rating: A:N

Vulnerability CVSS Score

Table 37. Null byte injection bypasses restriction filter CVSS score.

Scoring Date:	**N/A**	 **CVSS Calculator**
Base Score	**3.5**	
Impact Subscore	2.9	
Exploitability Subscore	6.8	
Temporal Score	**Not Defined**	
Overall Score	**3.5**	
		
Vector	(AV:N/AC:M/Au:S/C:P/I:N/A:N)	

5.5.4.9.1 Mitigations

Type filtering is done by Perl on the web server, but no syntax filtering is done. Filtering user data for null bytes would mitigate this vulnerability.

5.5.4.10 Security Concern

It is possible to insert a null byte for the display request, which will crash *webois.exe*. Since *webois.exe* is called once for every request, it is not possible to perform a DoS. Since no exploit was found with this method, it is a security concern.

5.5.4.11 Method Conclusions

Using the null byte injection in the URL to the web server, it is possible to bypass the restricted display filters. If a display is restricted by the display filter, a null byte injection bypasses this filter by altering the logic on the web server. It is also possible to crash the *webois.exe* process by sending a null byte for the display request. It is possible to mitigate this by filtering user input for null bytes and null byte encodings. Bounds checking should also be done in all code, particularly for *webois.exe* since a null byte crashed this service.

5.5.4.12 Method 5: Cookie Manipulation

Web users can also manipulate data in cookies. The Siemens TG web server cookies were tested for possible vulnerabilities introduced through cookie manipulation.

5.5.4.13 Vulnerability: DoS through Cookie Manipulation

Through cookie manipulation, it is possible to create a DoS of the Siemens TG web server service.

5.5.4.13.1 CVSS Base Metrics

Access Vector (AV)

The CVSS Access Vector rating is Network (N)—A vulnerability exploitable with network access means the vulnerable software is bound to the network stack, and the attacker does not require local network access or local access. Such a vulnerability is often termed "remotely exploitable." CVSS Rating: AV:N

Access Complexity (AC)

The CVSS Access Complexity rating is Low (L); specialized access conditions or extenuating circumstances do not exist. CVSS Rating: AC:L

Authentication (Au)

The CVSS Authentication rating is Single (S); one instance of authentication is required to access and exploit the vulnerability. CVSS Rating: Au:S

Confidentiality Impact (C)

The CVSS Confidentiality Impact rating is None (N); there is no impact to the confidentiality of the system. CVSS Rating: C:N

Integrity Impact (I)

The CVSS Integrity Impact rating is None (N); there is no impact to the integrity of the system. CVSS Rating: I:N

Availability Impact (A)

The CVSS Availability Impact rating is Complete (C); there is a total shutdown of the affected resource. CVSS Rating: A:C

Vulnerability CVSS Score

Table 38. DoS through cookie manipulation CVSS score.

Scoring Date:	**N/A**	 **CVSS Calculator**
Base Score	**6.8**	
Impact Subscore	6.9	
Exploitability Subscore	8	
Temporal Score	**Not Defined**	
Overall Score	**6.8**	
		
Vector	(AV:N/AC:L/Au:S/C:N/I:N/A:C)	

5.5.4.13.1 Mitigations

A temporary mitigation to this vulnerability is patching the Perl code responsible for parsing the cookies and limiting the length the *ClientID* value. A better mitigation would be to trace and locate which service is crashing and patch the root cause of the DoS. Since the service responsible for the DoS was not identified, further research is needed to determine which file(s) would need to be fixed.

5.5.4.14 Method Conclusions

It is possible to manipulate session cookies used to transmit data from host operating systems to the Siemens TG web server. By altering the *ClientID* cookie value, it is possible to create a DoS for the Siemens TG web server HMI service. It is unknown which service is ultimately responsible for the DoS, so a temporary fix would be to limit the size of the *ClientID* value in Perl. Once the service that is responsible for the DoS is identified, a patching the service is the best mitigation.

5.5.4.15 Method 6: Perform Hot Standby Swap via Web Interface

This method focused on the fact that the web interface was a read-only interface with no option of control. The goal of this method was to see if it is possible to perform a hot standby swap using the web interface. The hot standby swap is a control that is available when using the other HMI interfaces, but did not seem available to the web client. The ultimate goal was to see if an attacker could trick the web server to perform the hot standby swap.

Differences were checked between a typical HMI interface, as seen on *INLWS01*, and the web interface version, and it appeared that some functionality was missing or had been removed from the interface on *INLWEB*. Next, the method of installation was checked and found that there is a different install method between *INLWEB* and *INLWS01*. There are a number of *.DBIN* and *.menuscript* files missing from the directory *C:\lg\ws\dat\en_US*. Some of the missing *DBIN* and *menuscript* files are responsible for the control functionality seen missing on the web interface. After checking the log files

C:\lg\Post_Install_ReadMe.txt and *C:\powertg_installation.log*, it was concluded that the control functionality of the HMI on the *INLWEB* is missing because it is not installed by default and not built-in.

5.5.4.16 Security Concern

It was determined that the web interface may have the option of control even though it is not built-in. It may be possible to pass a DQS message through the web server to perform a Hot Standby Swap.

A hot standby swap was not accomplished in the testing performed during this assessment; however, the researchers are confident that given enough time the specific requirements applied to requests by the various programs that consume data from the *ProgReq.pl* script would be met, and arbitrary DQS messages would be possible.

It is strongly recommended that the ProgReq.pl script itself perform command filtering based upon the *allowed_requests.txt* file, only passing on requests that are explicitly authorized.

5.5.5 Conclusions

The web server on *INLWEB* was assessed with six different methods. Out of the six methods, three security concerns were found and four vulnerabilities were discovered.

One of the security concerns identified is a Perl script that prints out environment information that may be useful to an attacker. Another concern is the handling of null bytes in web languages and compiled code. Also tested was control through the web interface. It was determined that control on the web interface may be possible even though the functionality is not built-in. This may be accomplished by passing DQS messages though the web server, but more research is needed. Properly filtering user and/or external input will successfully mitigate the majority of the vulnerabilities and security concerns.

5.6 Target 6 – RTUCS Vulnerabilities

5.6.1 Introduction

This assessment activity will assess the RTUCS host of the Siemens Power TG system for vulnerabilities over the DNP. It will also focus on injecting data into the internal network from the RTU side of communications.

This section attempts to extract the pertinent information from the Cyber Researcher's report on AT6. The Cyber Researcher's report documents to a level where "someone similarly skilled in the art" can reproduce the results. This level is not required for the general report. For the reader that needs this level of detail, read the attached Cyber Researcher's report: Siemens Spectrum Power TG Cyber Report for AT6 – RTUCS.

5.6.2 Significance

This assessment target is significant due to it communicating with many units in the field. These units are not necessarily on a more secure network, and the RTUCS does not authenticate with them. Therefore, impersonating an RTU to inject specially formed or malicious data into the RTUCS could lead to possible compromise of the RTUCS, and possibly other connected systems on the Power TG network.

5.6.3 Assessment

For this assessment, the RTUCS server and its processes were targeted. The main objective was to explore the connection path between the RTU and the RTUCS, use fuzzing techniques to test the DNP handling for vulnerabilities, and test any secondary targets on the server. Secondary targets included any additional processes on the server, namely the *tg_rshserver* process.

5.6.3.1 Method 1: DNP 3.0 Fuzzing

The methodology and code used in Phase 1 was examined and improved upon for Phase 2. A DNP fuzzer was developed to impersonate an RTU to the level where the RTUCS would communicate with it on a continuous basis. This fuzzer was also made to test boundary conditions and possible attack scenarios when communicating with the RTUCS. Wireshark was heavily used to monitor and verify development progress on the fuzzer and the resulting responses from the RTUCS, as it has a reasonably mature dissector for the DNP.

A number of different DNP fields and functions were fuzzed. Attempts were made to cause a crash or overflow by sending invalid ranges, very large fragmented messages, and invalid transport layer values, along with other methods.

None of the fuzzing test cases caused a crash or overflow in the DNP handler processes. Either the RTUCS disconnected the RTU, or resent requests for data. The RTUCS seems to gracefully handle poor input.

5.6.3.2 Concern: Infinite Requests While Invalid Ranges Sent

While fuzzing, an attempt was made to send messages containing an invalid start-stop range, which was done by setting start higher than stop. Functionally, this should act as a negative range value and be invalid. The DNP handler processes on the RTUCS correctly reject these messages, but will request the information again until either manually told to offline the RTU or the RTU itself is taken offline. When reviewing the RTU panel on the Power TG workstation, the RTU is simply said to be online. This could be used as a way to sever the Power TG from one or several RTUs, but have the system show them to be operational.

5.6.3.3 Method Conclusions

Due to time and technical constraints, the fuzzer written could not fuzz the entirety of the DNP 3.0. Development was focused on creating a fuzzer that could emulate a RTU to a reasonable extent such that the RTUCS would communicate with it on a continuous basis, and then add in fuzzing functionality for the protocol. The fuzzer was used to verify a number of likely points of failure in the Power TG system's handling of the protocol, but none of the test cases resulted in a crash or other failure in the system.

Future evaluation should further validate message and flag-field combinations in the protocol. There are a large number of flags identifying various states within both the RTUCS and the RTU, and many combinations could not be tested due to time constraints.

5.6.3.4 Method 2: Source Code and Configuration Analysis

The configuration options for the Security Package were examined for this part of the assessment. Notably, SecurityConfig.xml was examined to see how commands were filtered by the *tg_rshserver*

program. This file led to an understanding of the filtering that the *tg_rsh* and *tg_rcp* programs use to prevent arbitrary command execution and filesystem access.

5.6.3.5 Zero-day Vulnerability: tg_rshserver Command Injection

Analysis of the configuration files for the common Power TG utilities (*tg_rsh*, *tg_rshserver*, *tg_rcp*, etc.) led to the discovery of mechanisms that control access to the *tg_rshserver* process.

5.6.3.5.1 CVSS Base Metrics

Access Vector (AV)

This vulnerability can be accessed remotely.

The CVSS Access Vector rating is Network (N)—A vulnerability exploitable with network access means the vulnerable software is bound to the network stack, and the attacker does not require local network access or local access. Such a vulnerability is often termed "remotely exploitable." CVSS Rating: AV:N

Access Complexity (AC)

Only certain commands are vulnerable to additional command injection. An attacker would have to find vulnerable commands, either by accessing the SecurityConfig.xml file, or through other means.

The CVSS Access Complexity rating is Medium (M); access conditions are somewhat specialized. CVSS Rating: AC:M

Authentication (Au)

An attacker would require a valid security certificate assuming the Power TG Security Package was installed. Otherwise, no authentication is required.

The CVSS Authentication rating is None (N); authentication is not required to access and exploit the vulnerability. CVSS Rating: Au:N

Confidentiality Impact (C)

Exploiting this vulnerability gives partial access to filesystem information, as the *tg_rshserver* drops privileges to another user when running commands.

The CVSS Confidentiality Impact rating is Partial (P); there is considerable informational disclosure. Rating C:P

Integrity Impact (I)

This vulnerability only provides some privileges to an attacker.

The CVSS Integrity Impact rating is Partial (P); modification of some system files or information is possible. CVSS Rating: I:P

Availability Impact (A)

An attacker does not have the available privileges to shut down the *tg_rshserver* process.

The CVSS Availability Impact rating is None (N); there is no impact to the availability of the system. CVSS Rating: A:N

Vulnerability CVSS Score

Table 39. tg_rshserver command injection CVSS score.

Scoring Date:	**N/A**	 **CVSS Calculator**
Base Score	**5.8**	
Impact Subscore	4.9	
Exploitability Subscore	8.6	
Temporal Score	**Not Defined**	
Overall Score	**5.8**	
		
Vector	(AV:N/AC:M/Au:N/C:P/I:P/A:N)	

5.6.3.5.1 Mitigations

Unfortunately, many of the commands that lack closing regular expression delimiters ('$') require arguments that are very hard to anticipate. Some commands have an expression that attempts to capture possible argument input, but these commands are more deterministic in their needs. The Power TG Security Package helps secure the *tg_rshserver* functionality somewhat by requiring cryptographic certificates to access it, but an internal attacker could still escalate his privileges (ex. from a workstation to a Power TG host) using this vulnerability. Requiring user credentials to use the *tg_rsh* / *tg_rcp* utilities, or using the *ssh / scp* programs would be a more secure alternative.

5.6.3.6 Method Conclusions

Analyzing the security configuration files lead to the discovery of a command injection flaw in the *tg_rshserver* process. While this flaw cannot be remotely exploited with the Security Package installed, deployments without the package are at risk. However, an internal attacker can still use this flaw to modify key files (workstation passwords, etc.) or obtain key information about the Power TG system, such as cryptographic certificates central to the system. The vulnerability found with this method affects all Power TG systems, as the *tg_rshserver* is a universal process in those systems.

5.6.4 Conclusions

The goals for this assessment were met, as the communications path between the RTU and the RTUCS was tested. Additional testing was also done on the *tg_rshserver* process, since it provides

another path into the RTUCS system. Work in this phase of the assessment did not expose any flaws in the DNP 3.0 handling, but more work could certainly be done in this area. The DNP is reasonably complex and deserves a more thorough treatment than could be done in the available time. Additionally, the *tg_rshserver* flaws represent a vulnerability that affects every Power TG server in a system, not just the RTUCS. Overall, the security posture for the RTUCS has improved since the Phase 1 assessment, especially in regards to the DNP, since no flaws granting administrative privileges were found this time.

6. ASSESSMENT SUMMARY

The purpose of this assessment was to identify vulnerabilities that exist in the Phase 2 configuration of the Siemens Power TG system and make recommendations to mitigate those vulnerabilities in the interest of protecting the critical infrastructure controlled by Power TG systems from cyber attack.

As listed in Section 4.3, and detailed in Section 5, this assessment found vulnerabilities in multiple categories as shown in Figure 3.

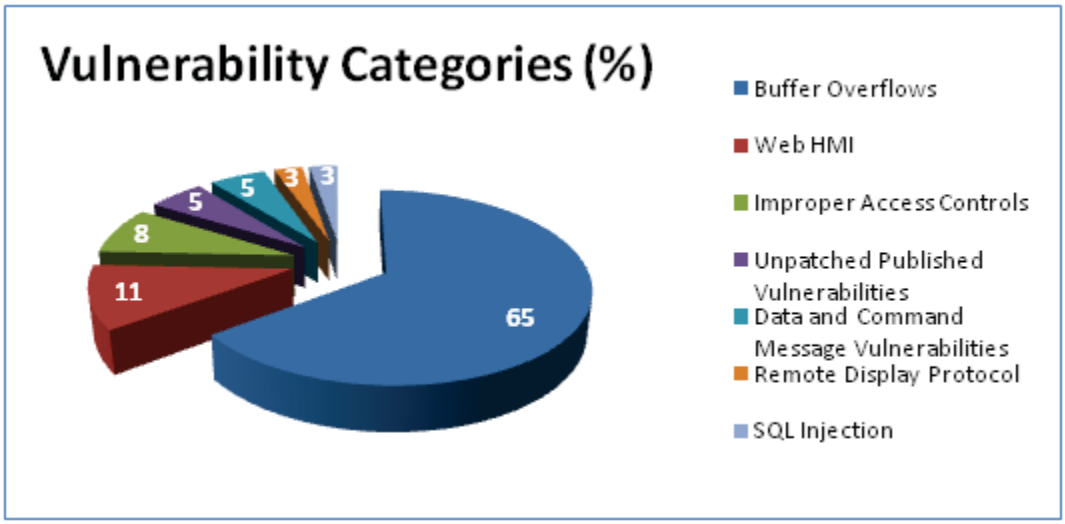


Figure 3: Assessment Vulnerability Category Breakdown

The vulnerability categories and associated mitigations that may be implemented to minimize their risk to this control system vulnerability are listed below:

- 65% of the vulnerabilities found in this assessment are buffer overflows, which can be by input validation;
- 11% of the vulnerabilities are Web HMI vulnerabilities, which can be mitigated by assessing how Web servers handle information provided by clients;
- 8% of the vulnerabilities are improper access controls vulnerabilities (authorization), which can be mitigated by locking down all applications, hosts, and networks to limit the consequences of compromise as much as possible;
- 5% of the vulnerabilities are unpatched published vulnerabilities, which can be mitigated by routinely assessing all SCADA components, including operating systems, applications, services, network devices, etc., for published vulnerabilities;
- 5% of the vulnerabilities are SCADA data and command message manipulation and injection vulnerabilities, which can be mitigated by redesigning SCADA network protocols and the service applications that implement them for security;

- 3% of the vulnerabilities is the use of vulnerable remote displays protocols, which can be mitigated by minimizing usage, exposure, and available functionality of remote display protocols; and

- 3% of the vulnerabilities is an SQL injection vulnerability, which can be mitigated by protecting SCADA databases through input validation and filtering.

In addition to these vulnerabilities, the team also found noteworthy security practices and improvements in the Power TG system since the conclusion of Phase 1 testing. As mentioned in the Executive Summary, and as fully detailed in Section 5, the team found the following: important vulnerabilities from Phase 1 were resolved; firewall rules were improved and more consistent; important processes no longer allow improper administrative privileges; Power TG servers have fewer unnecessary services running, and remaining extraneous services have been firewalled from external access; a newer version of Microsoft Terminal Services resolved a previous vulnerability; the optional security package for the Power TG system was implemented well and should come standard with the system; the security posture for the RTUCS system has improved; and, overall, the security and quality of coding practices have improved.

Although several important vulnerabilities from Phase 1 testing were resolved, others have yet to be mitigated, and new vulnerabilities requiring further mitigation were found in Phase 2. Overall, the Siemens Power TG system's development spans a period of time that has seen concern over secure coding practices go from low to very high. The system's newer code generally adheres to secure coding practices while older sections of the system do not. In addition to mitigating the remaining vulnerabilities from Phase 1 and the new vulnerabilities from Phase 2, it is strongly recommended that the Power TG's older code base be refactored or rewritten in accordance with a more modern concern for secure coding practices.

7. AFTER ACTION REPORT

An After Action Report (AAR) is required from Siemens to document the mitigations and improvements made to the Siemens Basic System Platform based on the cyber security assessment in regard to control system security. This information provides a valuable metric on the relative progress that DOE-OE's Cyber Security for Energy Delivery Systems R&D program is making in respect to securing the control systems deployed in the Energy sector. The AAR will include the identified vulnerabilities, actions taken for mitigation, patches developed and deployed, full system deployments with updated security measures based off the findings, and any alerts or bulletins that were delivered to the vendors' user communities for awareness. If an identified vulnerability was not addressed, DOE-OE would like to know what your path forward is to address it.

7.1 Products

A final AAR will be provided to DOE-OE through the Assessment Lead, on mitigation and security practices implemented to address the vulnerabilities that were identified in this assessment report. Content of the AAR will include:

- Identified vulnerability
- Vulnerability ranking
- Action taken for each vulnerability
- Patches developed and deployed for vulnerabilities
- Increased security practices/technologies within the product line
- Alerts and bulletins
- Vulnerabilities not addressed and path forward to mitigate.

7.2 Deliverable Schedule/Process

The delivery schedule and process must be followed to secure the information and provide a status update on actions taken to reduce the risk to critical infrastructure and provide more secured systems to industry.

The AAR is due 6 months after the original delivery date of the assessment report. A secured delivery of the AAR will be required to protect the data; Pretty Good Privacy is a preferred method with key exchange to provide for encryption capabilities.

INL/LTD-11-23857

Siemens Spectrum Power 3 System Cyber Security Assessment Report

October 2011

Assessment Team Performers List
Trent Taylor
Robert Erbes
Kent Kvarfordt
James Thomas
May Chaffin
Nate Bowman
Zack Adams

Idaho National Laboratory

The INL is a U.S. Department of Energy National Laboratory
operated by Battelle Energy Alliance

EXECUTIVE SUMMARY

The goal of the U.S. Department of Energy Office of Electricity Delivery and Energy Reliability (DOE-OE) National Supervisory Control and Data Acquisition (SCADA) Test Bed (NSTB) program is to enhance the reliability and resiliency of the nation's energy infrastructure by reducing the risk of energy disruptions due to cyber attacks. A key part of the program is SCADA system vulnerability analysis that identifies and provides mitigation approaches for vulnerabilities that could put these systems at risk. A cyber security vulnerability is a weakness in a computing system that can result in harm to the system or its operation, especially when this weakness is exploited by a hostile actor or is present in conjunction with particular events or circumstances.

In 2006, DOE collaborated with energy owners and operators to develop a strategy to secure energy control systems going forward, made available through the Roadmap to Secure Control Systems in the Energy Sector. In 2011 the Roadmap was updated to keep pace with advances in technology and the evolving threat landscape and renamed the Roadmap to Achieve Energy Delivery Systems Cyber Security. The Roadmap lays out a vision that by 2020, resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions. One of the Roadmap strategic directions needed to achieve this vision is to assess and monitor risk, which is the subject of this report.

A cyber security research team from Idaho National Laboratory (INL) performed a cyber security assessment of the Siemens Power Transmission and Distribution (PT&D) Spectrum Power 3 system in the INL test bed from July 24 until November 15, 2011. The purpose of this assessment was to understand vulnerabilities that exist in the Power 3 system and make recommendations to mitigate those vulnerabilities in the interest of protecting the critical infrastructure controlled by Power 3 systems from a cyber attack.

The Phase 2 cyber security assessment performed by INL was focused on a set of assessment targets developed in conjunction with Siemens PT&D personnel. Assessment targets reflect steps an actual attacker may take to gain control of the Power 3 system and cause damage to customers, employees, equipment, and competitive ability, in addition to those who rely on Power 3 system operations.

During the cyber assessment, the team recognized that the Power 3 system has the following noteworthy security practices:

- Important vulnerabilities identified in Phase 1 testing were successfully mitigated (though several have not been mitigated)
- The Spectrum Power 3.10 hosts in Phase 2 testing have fewer services listening on the network than the Spectrum Power 3.9 hosts in Phase 1, which makes them less exposed to attack
- The implementation of the Web Human-Machine Interface (HMI) appears to have been implemented well (with several notable exceptions, which are detailed in Section 5)

- The implementation of the Secure Socket Layer (SSL), on which the majority of Power 3 protocols now lay, was found to be generally well implemented.

The assessment found that the Power 3, as configured for this assessment, has a number of vulnerabilities associated with the planned Assessment Targets that may facilitate a successful cyber attack. The items listed below identify vulnerability categories, the number of occurrences, and the range of scores showing where the occurrences fall on the Common Vulnerability Scoring System (CVSS):

- Buffer Overflows in SCADA Services (15 instances, each with a CVSS score 9.3)
- Denial of Service (DoS) (nine instances, with CVSS scores ranging from 4.3 to 7.8)
- Improper Access Controls (Authorization) (four instances, with CVSS scores ranging from 3.0 to 7.3)
- Unpatched Published vulnerabilities (one instance, with a CVSS score of 7.8)
- Web HMI vulnerabilities (one instance, with a CVSS score of 4.3)
- SCADA Data and Command Message Manipulation and Injection (one instance, with a CVSS score of 9.3)
- Structured Query Language (SQL) Injection (one instance, with a CVSS score of 6.9).

A complete listing of all individual vulnerabilities can be found in Section 4.3.

Recommendations for mitigating the risk of the cyber attacks detailed in this report include the following:

- Mitigate buffer overflow and DoS vulnerabilities by performing input validation, a core component of secure source code development.
- Mitigate improper access controls by locking down all applications, hosts, and networks to limit the consequences of compromise as much as possible.
- Mitigate unpatched published vulnerabilities by routinely assessing all SCADA components, including operating systems, applications, services, network devices, etc., for published vulnerabilities, patching any vulnerabilities identified.
- Mitigate Web HMI vulnerabilities by assessing Web servers with regards to how client input is handled and filtered. Special attention should be paid to web servers that allow access to the physical system.
- Mitigate SCADA data and command message manipulation and injection by redesigning SCADA network protocols and the service applications that implement them for security.
- Mitigate SQL injection by protecting SCADA databases. Follow the principle of least privilege. Use the strictest permissions possible on all database objects, such as execute-only for stored procedures.

Overall, the team found that most vulnerabilities from Phase 1 testing have been mitigated; however, new vulnerabilities requiring further mitigation were found in Phase 2. In addition, the team also found noteworthy security practices and improvements in the Power 3 system since the conclusion of Phase 1 testing. Further details on the new vulnerabilities and improvements in the Phase 2 test system are found in Section 5.

Finally, the Power 3 System has shown a positive progression toward secure systems. This is evident not only by the patches implemented in Phase 2 that fix vulnerabilities identified in Phase 1, but also in the security architecture that has been implemented. However, it is strongly encouraged that Siemens continue the process of security assessments and testing.

CONTENTS

FIGURES

TABLES

ACRONYMS

AAR	After Action Report
ADM	Administrator
API	Application Programming Interface
ARP	Address Resolution Protocol
AT	Assessment Target
BaSiWi	Basic Signaling Window
BDP	Basic Data Processing
BSW	Basic Signaling Window
CA	Communications Application
CFE	Communications Front End
CIP	Critical Infrastructure Protection
COM	Communicator
CPU	Central Processing Unit
CVE	Common Vulnerability Exposure
CVSS	Common Vulnerability Scoring System
DAqS	Data Acquisition System
DMZ	Demilitarized Zone
DNP	Distributed Network Protocol
DNP3	Distributed Network Protocol Version 3
DNS	Domain Name Server
DOE	U.S. Department of Energy
DOE-OE	Department of Energy Office of Electricity Delivery and Energy Reliability
DoS	Denial of Service
EMS	Energy Management System
FTP	File Transfer Protocol
HIS	Historical Information System
HMI	Human-Machine Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICCP	Intercontrol Center Communications Protocol
ICS	Industrial Control System
INL	Idaho National Laboratory
IP	Internet Protocol

JDBC	Java Database Connectivity
LAN	Local Area Network
MitM	Man-in-the-Middle
MMI	Man-Machine Interface
MMS	Manufacturing Messaging Standard
NA	Network Analysis
NERC	North American Electric Reliability Corporation
NFS	Network File System
NIM	Network Image
NSTB	National SCADA Test Bed
OSI	Open System Interconnection
OWASP	Open Web Application Security Project
PDM	Primitive Data Manager
PT&D	Power Transmission and Distribution
RFE	Remote Front End
RSH	Remote Shell
RTDS	Real-Time Data Server
RTU	Remote Terminal Unit
SBXFER	Softbus Shared Memory Transfer
SCADA	Supervisory Control and Data Acquisition
SISCO	Systems Integration Specialists Company, Inc.
SPM	Switching Procedure Management
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TNA	Transmission Network Apps
UCS	Utility Communications Server
UDP	User Datagram Protocol
UI	User Interface
URL	Uniform Resource Locator
VIOS	Virtual I/O Server
XSS	Cross Site Scripting

PART 1 – ASSESSMENT PROCESS

1 INTRODUCTION

The U.S. Department of Energy (DOE) established the National Supervisory Control and Data Acquisition (SCADA) Test Bed (NSTB) program to help industry and government improve the security of control systems used in the nation's energy infrastructures. The NSTB is funded and directed by the DOE Office of Electricity Delivery and Energy Reliability (DOE-OE). A key mission of the program is to assess control systems for vulnerabilities that could put critical infrastructures at risk from cyber attack.

This report describes the Idaho National Laboratory (INL) cyber security assessment of the Siemens Power Transmission and Distribution (PT&D) Spectrum Power 3 Version 3.10 (hereafter referred to as Power 3) system conducted in the INL Test Bed from July 24 until November 15, 2011. The Power 3 system has been designed specifically for utility networks.

1.1 Assessment limitations

This report represents an attempt to assess the most critical vulnerabilities that could put the Power 3 control system at risk for a cyber attack. However, it is not intended to provide a complete assessment of all the vulnerabilities associated with the Power 3 control system. Furthermore, the findings and recommendations presented herein do not consider or determine compliance with National Electric Reliability Council (NERC) Critical Infrastructure Protection (CIP) Standards.

The observations and recommendations in this report are based on common security practices and the experience of the assessment team. The team does not claim to understand all of the issues affecting operation, maintenance, and architecture of the Power 3 control system. Observations and recommendations made as a result of this assessment may not take into account mitigations already in place. It is also possible that operational requirements preclude implementation of some recommendations.

The assessment was performed on a Power 3 system configured by Siemens to represent a typical baseline installation. No asset owner was involved in the system configuration, and the configuration does not represent any one facility. The assessment system does not include the network devices and perimeters typically found in an actual user's installation.

2 ASSESSMENT METHODOLOGY

The methodology used for the Power 3 system cyber security assessment includes the following activities:

- Control system target selection

  Together with Siemens personnel, the assessment team identifies a list of assessment targets. These targets are specific objectives for which Siemens requested review, along with those identified to be of strategic interest to potential attackers. These targets provide the basis for subsequent assessment activities.

- Identification of vulnerabilities in selected targets

  Using a combination of commercial, proprietary and open-source tools, the cyber assessment team discovers information about the targets that may allow the assessment team to compromise the pre-defined targets. During the course of this discovery, the assessment team may also identify additional targets.

  By documenting their course of action and the results of each activity, the assessment team characterizes the vulnerabilities as Day Zero, Published, or Configuration Induced vulnerabilities.

  Definitions:

  Day Zero Vulnerability. A vulnerability discovered during the assessment that has no published corollary.

  Known Vulnerability. A published vulnerability as defined by its definition in the Common Vulnerability Exposure (CVE[1]) database.

  Configuration-Induced Vulnerability. A vulnerability that is created as a result of some configuration issue that may be resolve using best or recommended practices.

- Identify or develop a proof-of-concept or exploit associated with the identified vulnerabilities

  With the information gleaned from antecedent activities, the cyber assessment team attempts to exploit the vulnerabilities they have identified. If a full exploit is not cost effective, proof-of-concept code for an exploit may be developed.

- Metrics Scoring

  Using the research information, scoring metrics based on the Common Vulnerability Scoring System[2] (CVSS) are added to provide a metrics methodology for comparison with vulnerabilities from other sources based on a common methodology.

- Recommendations for remediation of identified vulnerabilities

  Having characterized the identified vulnerabilities, the assessment team provides their best recommendation to remediate the vulnerabilities. These recommendations are based primarily on the experience of the assessment team, and may not be feasible or reflect the operational constraints of the process control system, but should be considered as part of the reader's risk management process.

1. CVE: Common Vulnerability Exposure at http://cve.mitre.org/.
2. CVSS 2.0 Guide: http://www.first.org/cvss/cvss-guide.pdf.

3 SYSTEM DESCRIPTION

As described in Steps 1 and 2 of the Assessment Methodology section, the assessment team first sought to understand the system to be assessed and to identify assessment targets. This section includes the system architecture, diagrams, and descriptions to provide the reader context for the vulnerabilities identified during this assessment.

3.1 System Architecture

The system architecture consisted of two physical computers: a Virtual I/O Server (VIOS), which was an IBM Server, and an IBM desktop computer that runs Windows XP as an operating system. The VIOS server was configured to run seven virtual machines, which consisted of a Data Management Server (AD1INL), Real-time Communicator (CM1INL), Network Analysis server (NA1INL), Utility Communication Server (UC1INL), Communication Front-End Server (CF1INL), Remote Front-End Server (RF1INL), and User Interface (UI) Server (MM1INL). The standalone computer was configured as a workstation and UI client.

The system provided by Siemens for the assessment is shown below in Figure 1.

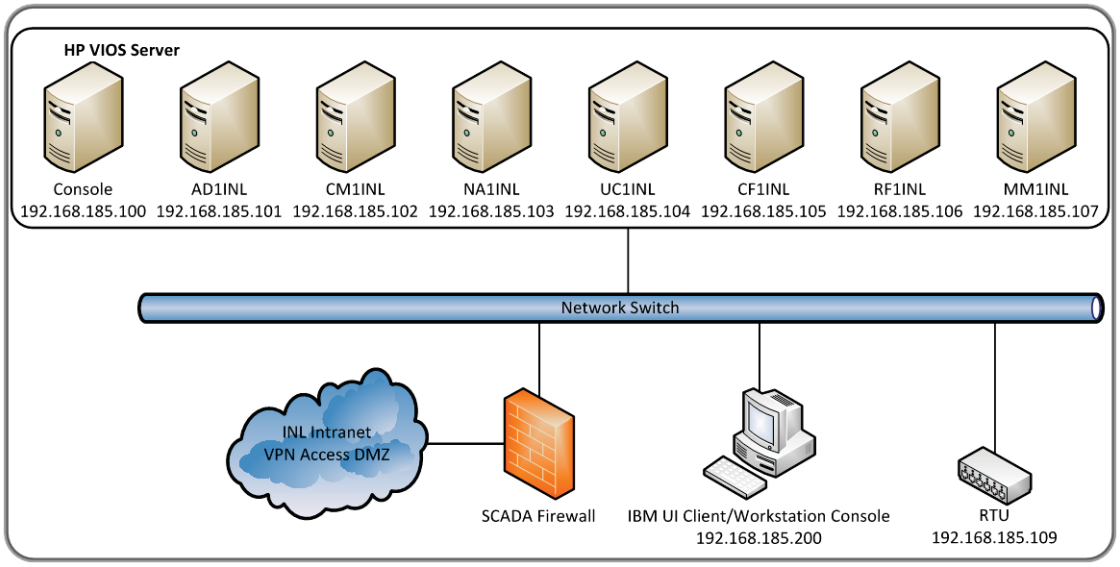


Figure 1. Siemens Spectrum Power 3.10 assessment system.

On the IBM VIOS server resides, used to perform administrative task the Administrator (ADM) server (AD1INL) runs an AIX operating system. The Communicator (COM) server (CM1INL) runs under an AIX operating system and is used to process data on the Energy Management System (EMS). The Network Analysis (NA1INL) server runs under the AIX operating system and is used to provide scheduling and analysis on the EMS network. A VIOS running AIX was configured as a Utility Communications Server (UCS) server (UC1INL), which is used for inter control center communication. Siemens Power 3 Communications Front End (CFE) server (CF1INL) running on an AIX operating platform is used as the interface to allow data exchange between Remote Terminal Units (RTUs) of different providers and Power 3. The Remote Front End (RFE) server (RF1INL) provides the same functions as the CFE but provides remote connectivity. The Man-Machine Interface (MMI) server (MM1INL) was an AIX VIOS and served as the UI client for the EMS. The standalone desktop computer running a Windows XP operating system served as a second workstation (IBM UI) and was also configured as interface to the IBM VIOS server. The final component in the system was a Station Manager RTU that was configured to handle digital and analog inputs and outputs that could be modified using the Configuration Management Program, CMP975.

Networking for the assessment consisted of a single network with Internet Protocols (IPs) ranging from 192.168.185.100-109.

3.2 Major Components

The ADM server and/or the ADM spare server are used to perform administrative tasks in the systems. They manage the database maintenance processes, and they are often used to hold the AIX installation files.

3.2.1 AD1INL

3.2.1.1 Core Functions

Server Function – RDBMS Interface, Database Administration, Graphic Editor, Historical and Future Data, Load Forecast, Interchange Transaction Scheduler, Outage Scheduler.

3.2.2 CM1INL

The COM Server is used to process data on the Energy Management System. The dynamic master block function for the process data base files is the COMM, which runs on the COM. Current switching statuses are process data, which are stored in a data base file on COM.

3.2.2.1 Core Functions

Server Function – SCADA, AGC, and MultiSite Functions.

3.2.3 NA1INL

The Network Analysis (NA) server is used to provide scheduling and analysis on the EMS network. There are a variety of applications that are run on the NA and are listed below:

- Fault Calculation (FC)
- Network Sensitivity (NS)
- Network Parameter Adaptation (PA)
- Security Analysis (SA)
- Security Constrained Economic Dispatch (SD)
- State Estimator (SE)
- Security Analysis Look Ahead (SL)
- Voltage Scheduler (VS).

3.2.3.1 Core Functions

Server Function – Scheduling Applications, Network Analysis Applications, excluding Outage Scheduler.

3.2.4 UC1INL

Data is received from the field devices by the Data Acquisition System (DAqS) or received from other control centers by the UCS and is passed to the Realtime COM for processing. Request may come from a local UI server, from a remote control center through the UCS server.

3.2.4.1 Core Functions

Server Function – ELCOM Data Link, ICCP Data Link, and WSCC Data Link

3.2.5 CF1INL

The CFE is an AIX-based process interface designed to allow data exchange between RTUs of different providers and Power 3.

3.2.5.1 Core Functions

Server Function – Data Acquisition and Supervisory Control RTU/field device Interface

3.2.6 RF1INL

The RFE is an optional server-based system that allows the user to have a connection to the RTUs that is remote from the CFEs. That is, the CFEs are typically configured in the control center, whereas the RFEs may be miles from and independent of a control center.

3.2.6.1 Core Functions

Server Function – Data Acquisition and Supervisory Control RTU/field device Interface

3.2.7 MM1INL

The MMI servers are used to manage the EMS from "operator consoles" (also called "dispatcher consoles"). WorldMap Windows (also referred to as One-lines) are the portions of the UI that are used most often. They are used for displaying One-line diagrams and some application displays.

3.2.7.1 Core Functions

Server Function – User Interface

3.3 System Operation

Normal startup operations for the Power 3 system was for the VIOS server machine to power on and a script will run to start all of the VIOS servers: AD1INL, CM1INL, NA1INL, UC1INL, CF1INL, RF1INL, and MM1INL. The EMS system can also be manually stopped and started running the scripts. The standalone Windows XP machine can be powered on, a script will run to start the UI, and from the running workstation the operator can access the Power 3 VIOS server and select individual VIOS servers. Each of the above listed VIOSs had a snapshot taken after configuration and proper operations were tested. The snapshot for the VIOSs provided a quick backup and recovery process for the majority of the Power 3 software and configuration. The standalone machine, which had the second UI and client, was cloned for backup and recovery needs.

With all of the backups taken and stored on a separate storage device in a secure area, the team would be able to recover any part or the entire system if needed. To perform a restore to any or all of the system the Power 3 system would be stopped, images restored as needed, and the startup process as stated above could be used to return the system to a desired operating status.

PART 2 – ASSESSMENT RESULTS

4 ASSESSMENT OVERVIEW

The initial tasks for this assessment focused on specific Assessment Targets (AT) agreed upon by Siemens and the assessment team. These ATs, shown in Table 1, are based on goals of a real attacker to exploit the control system and cause damage to equipment, service, or users. The initial goals outlined are prioritized based on their potential impact to an installed Siemens system.

Table 1. Assessment Targets (ATs).

Target No.	Target Objective	Target Description
1	User Interface Server	"MMI" Power 3 Block Function where the JBOSS webserver and TIBCO SmartSockets server runs and Data Servers
2	Communications Front-End and Remote Front-End Servers	RTU protocol stacks
3	Communication Protocols	ADM Server – All Power 3 apps access the ADM static configuration Oracle Database, Certificate Authority, Historical Information System (HIS) Oracle database resides on the ADM server
4	Communicator Server	Data Servers
5	Applications that Access Oracle	Escalation of privileges, Structured Query Language (SQL) injection attacks, etc and ADM server - All Power 3 apps access the ADM static configuration Oracle Database
6	Utility Communications Server	ICCP protocol
7	Phase 1 Patch Validation	Evaluate any patches or fixes to the software that resolve issues identified in the Phase 1 Assessment

4.1 Metrics

Metrics are an important part of vulnerability assessments. Metrics provide a common methodology for evaluating vulnerabilities. With well developed and common metrics, end users have a common base for vulnerability.

Vulnerability research teams assessing Industrial Control Systems (ICS) and their components use the CVSS.[3] These metrics are evaluated for all vulnerabilities identified in this report.

CVSS is composed of three metric groups: Base, Temporal, and Environmental, each consisting of a set of metrics, as shown in Figure 2.

3. CVSS 2.0 Guide: http://www.first.org/cvss/cvss-guide.pdf, date last accessed November 8, 2011.

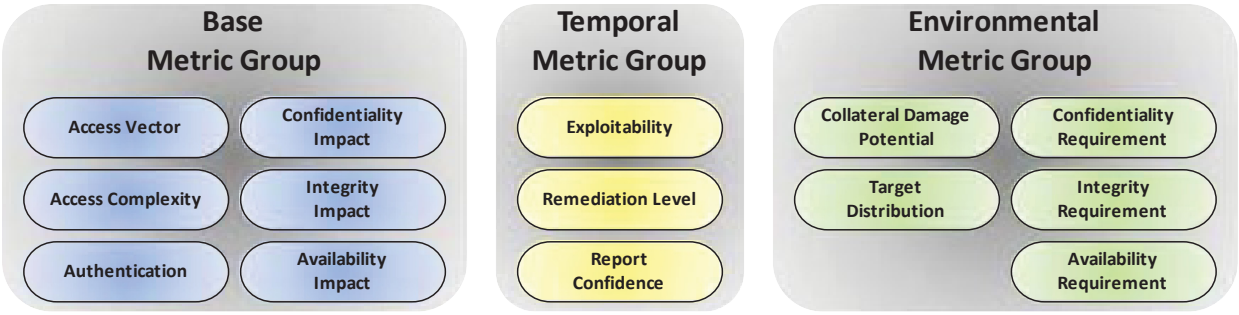


Figure 2. CVSS metric groups.

These metric groups are described as follows:

- Base. Represents the intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments.
- Temporal. Represents the characteristics of a vulnerability that change over time but not among user environments.
- Environmental. Represents the characteristics of a vulnerability that are relevant and unique to a particular user's environment.

The purpose of the CVSS base group is to define and communicate the fundamental characteristics of a vulnerability. This objective approach to characterizing vulnerabilities provides users with a clear and intuitive representation of a vulnerability.

The purpose of the CVSS temporal group is to define the state of the vulnerability at the time this research document was published. Since it is time dependent, the metric scoring may change after publication. The end user should review this score in the context of the elapsed time since publication as the scores for this group may have changed.

The purpose of the CVSS environmental group is to provide contextual information that more accurately reflects the risk to an end user's unique environment. This group of metrics is beyond the scope of this research document. The end user should score the environmental metric group based on their installation. This allows them to make more informed decisions on prioritization when trying to mitigate risks posed by the vulnerabilities based on the operational consequences of their installation.

4.2 Example CVSS Scoring

The CVSS scores for vulnerabilities identified in this report are, generated using the National Vulnerability Database calculator. An example of this scoring is shown in Table 2. The CVSS Calculator icon contains a hotlink to this calculator with the values in the table automatically entered. This calculator provides the reader the option to score the Environmental Metrics. Adding the Environmental Metrics will assist the end use in vulnerability evaluation and mitigation prioritization.

Table 2. Sample vulnerability CVSS score.

Scoring Date:	**N/A**	
Base Score	**6.9**	 **CVSS Calculator**
Impact Sub score	8.5	
Exploitability Sub score	5.5	
Temporal Score	**Not Defined**	
Overall Score	**6.9**	
		
Vector	(AV:A/AC:M/Au:N/C:P/I:P/A:C)	

4.3 Vulnerability Summary

This section integrates the findings from the assessment into a tabular format, shown in Table 3, to identify the critical results quickly. They are sorted based on the CVSS overall score.

This sorting does not take into account the operational consequences associated with the vulnerabilities presented. To properly evaluate these consequences the reader should evaluate the environmental metrics group for their installation and use the updated score to assist in evaluating the risks associated with the vulnerability in their installations.

A full understanding of each vulnerability listed requires that the applicable document section be carefully reviewed. Only through an understanding of the vulnerability can the reader use this information to establish the operational consequences associated with their installation.

Table 3. Summary of vulnerabilities, ratings, assessment targets, and affected components.

Vulnerability	CVSS Overall Score	AT No.	Affected SCADA/EMS Components
Hummingbird HostExplorerTerminal "Organization" Buffer Overflow (ActiveX vulnerabilities with 9.3 CVSS score)	9.3	1	User Interface
Hummingbird HostExplorerTerminal "GetToolbar" Buffer Overflow (ActiveX vulnerabilities with 9.3 CVSS score)	9.3	1	User Interface
Hummingbird HostExplorerTerminal "LoadDocfile" Buffer Overflow (ActiveX vulnerabilities with 9.3 CVSS score)	9.3	1	User Interface
Hummingbird PrintExplorerCtrl "SavePrinterProfile" Buffer Overflow (ActiveX vulnerabilities with 9.3 CVSS score)	9.3	1	User Interface

Table 3. (continued).

Vulnerability	CVSS Overall Score	AT No.	Affected SCADA/EMS Components
Hummingbird PrintExplorerCtrl "Host" Buffer Overflow (ActiveX vulnerabilities with 9.3 CVSS score)	9.3	1	User Interface
Hummingbird PrintExplorerCtrl "LUName" Buffer Overflow (ActiveX vulnerabilities with 9.3 CVSS score)	9.3	1	User Interface
Hummingbird PrintExplorerCtrl "CodeBaseURL" (ActiveX vulnerabilities with 9.3 CVSS score)	9.3	1	User Interface
Hummingbird PrintExplorerCtrl "DisplayProfile" (ActiveX vulnerabilities with 9.3 CVSS score)	9.3	1	User Interface
Hummingbird PrintExplorerCtrl "HTMLFileTitle" (ActiveX vulnerabilities with 9.3 CVSS score)	9.3	1	User Interface
Hummingbird PrintExplorerCtrl "PrinterProfile" (ActiveX vulnerabilities with 9.3 CVSS score)	9.3	1	User Interface
Hummingbird HCLXWebHostCtrl "PlainTextPassword" (ActiveX vulnerabilities with 9.3 CVSS score)	9.3	1	User Interface
Hummingbird HCLXWebHostCtrl "Src" (ActiveX vulnerabilities with 9.3 CVSS score)	9.3	1	User Interface
Microsoft WebBrowser "ReadyState" (ActiveX vulnerabilities with 9.3 CVSS score)	9.3	1	User Interface
Arbitrary Code Execution with RfeMaster	9.3	2	RFE
dsiServer Stack Based Buffer Overflow	9.3	3	ADM
MMS Layer Block 4 Message Heap Overflow	9.3	6	ICCP
RfeMaster Denial of Service	7.8	2	RFE
Sisco OSI Stack TPKT Layer Denial of Service	7.8	6	ICCP
Power 3 files accessible via NFS	7.3	4,7	ADM, COM, TNA, UCS, CFE
MMS Layer Invalid Pointer Dereference	7.1	6	ICCP
MMS Layer Block 4 Message Unhandled Memory Allocation Denial of Service	7.1	6	ICCP
Large Outstanding Requests Denial of Service	7.1	6	ICCP
MMS Layer Invalid Local Detail Denial of Service	7.1	6	ICCP
BULS DoS Vulnerability	7.1	7	All
SQL injection	6.9	5	All
Bypass the Power 3 Application Logon Process	6.8	1	User Interface
Hummingbird PrintExplorerCtrl "Connected" (ActiveX vulnerabilities with 4.3 CVSS score)	4.3	1	User Interface

Table 3. (continued).

Vulnerability	CVSS Overall Score	AT No.	Affected SCADA/EMS Components
Microsoft WebDVDDeviceSegment "AcceptParentalLevelChange" (ActiveX vulnerabilities with 4.3 CVSS score)	4.3	1	User Interface
Microsoft WebDVDDeviceSegment "StillOff" (ActiveX vulnerabilities with 4.3 CVSS score)	4.3	1	User Interface
Logon Token Cross-Site Scripting (XSS)	4.3	1	User Interface
Password Database Decryption	3.0	2	All

5 ASSESSMENT TARGETS

Assessment Targets (ATs) were identified in conjunction with Siemens personnel prior to the hands-on portion of the assessment and represent steps an attacker might take to compromise the system. This section provides an overview of each assessment target's results. Further details for each AT are in the embedded cyber security reports included in each subsection. These embedded reports were written as stand-alone documents with the goal of recording the process such that someone similarly "skilled in the art" could reproduce the results. Figure 3 illustrates how all data flows through the Power 3 system.

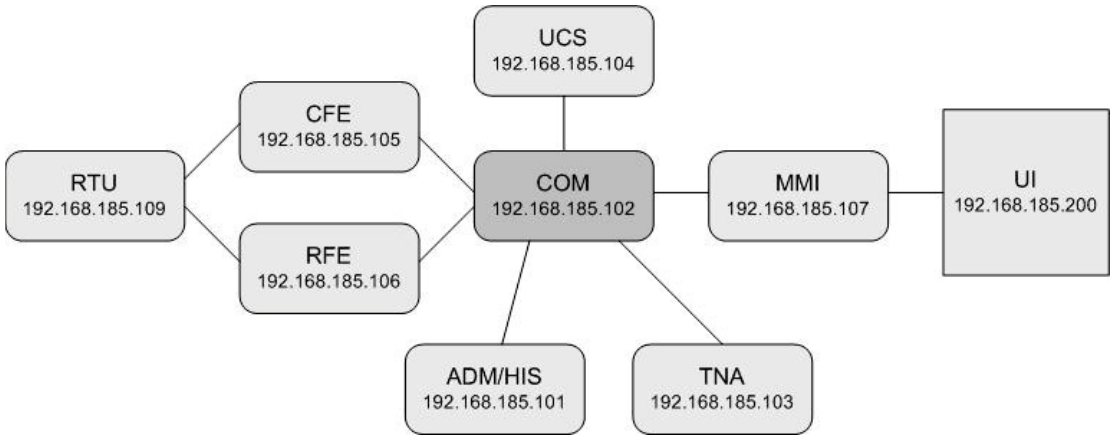


Figure 3. SCADA dataflow of the INL Power 3 system.

5.1 Target 1 – User Interface Server

5.1.1 Introduction

The Siemens Power 3 is an energy management solution for the automation, control, and protection of power transmission and distribution. In the current version of Power 3, a UI server provides a Web-based UI. The UI consists of the following components:

- Basic Signaling Window (BSW or BaSiWi). The entry point to all Power 3 applications.
- WorldMap Window. Also referred to as One-lines; used for displaying One-line diagrams and some application displays.
- Applications, Utilities, and Miscellaneous Displays. Power 3 includes a number of applications, utilities, and miscellaneous displays (e.g., Transmission Network Applications, Historical Information System, CurveTool, and Station Tabular application).

For this assessment, the configuration of the UI server software consists of a JBoss Application Server,[4] TIBCO SmartSockets,[5] as well as the Stunnel[6] software. The Web-based UI consists of Windows Internet Explorer, ActiveX7 components, Scalable Vector Graphics,[8] HTML, and JavaScript.

4. JBoss Application Server http://en.wikipedia.org/wiki/JBoss_application_server, date last accessed November 8, 2011.
5. TIBCO SmartSockets http://www.tibco.jp/software/messaging/smartsockets/default.jsp, date last accessed November 8, 2011.
6. Stunnel http://en.wikipedia.org/wiki/Stunnel, date last accessed November 8, 2011.
7. ActiveX http://en.wikipedia.org/wiki/ActiveX, date last accessed November 8, 2011.
8. Scalable Vector Graphics http://en.wikipedia.org/wiki/Scalable_Vector_Graphics, date last accessed November 8, 2011.

This section attempts to extract the pertinent information from the Cyber Researcher's report on AT1. The Cyber Researcher's report documents to a level where "someone similarly skilled in the art" can reproduce the results. This level is not required for the general report. For the reader that needs this level of detail, read the attached Cyber Researcher's report: AT1 – User Interface Server.


AT1 - User Interface Server.pdf

5.1.2 Objective

The objective of this section of the assessment is, from a presence on the trusted network, to compromise the ability of the Power 3 UI server to function as expected and to investigate and exploit attack vectors and vulnerabilities exposed by the UI server and Web-based UI.

5.1.3 Significance

The unauthorized disruption or manipulation of the UI server and Web-based UI may lead to loss of control, loss of data, disruption of service, or a malfunction of the device.

5.1.4 Rules of Engagement

Source code was not provided for this assessment. There were no other restrictions.

5.1.5 Assessment

The assessment target for this section of the report is the Power 3 UI server and Web-based UI. This assessment investigates and exploits attack vectors and vulnerabilities exposed by the configuration, implementation, and network communications of the UI server and Web-based UI.

5.1.5.1 Method 1: ActiveX Control Fuzzing

This method focuses on the ActiveX controls installed on the IBM UI Client/Workstation Console (192.168.185.200 – Windows UI). Vulnerable ActiveX controls could allow an attacker to gain control of this part of the system. Most commonly, an attacker can leverage vulnerable ActiveX controls by enticing a user to visit a malicious website in which the control is exploited to gain remote access to the IBM UI Client/Workstation Console. Vulnerable ActiveX controls can also be exploited through Internet banner ads or malicious websites to which a user may casually browse. Thus, Internet connectivity to the IBM UI Client/Workstation Console is a requirement for an attack originating outside the local network. Without Internet connectivity, an attack would still be possible from any system on the same local network as the IBM UI Client/Workstation Console. However, this greatly reduces the attack surface of the vulnerability.

There are 16 ActiveX control vulnerabilities, thirteen of which have a CVSS score of 9.3, and three with a CVSS score of 4.3. The ActiveX control vulnerabilities with the same CVSS score are listed together, with each group followed by the applicable set of CVSS baseline metrics and the applicable CVSS scoring table. Vulnerabilities with a score of 9.3 are listed first and those with a score of 4.3 are listed second, followed by mitigations for all 16 ActiveX control vulnerabilities, under the heading "Method 1 Mitigations."

ActiveX Vulnerabilities with 9.3 CVSS Score

1. **Zero Day Vulnerability: Hummingbird HostExplorerTerminal "Organization" Buffer Overflow**

   If an attacker sets an overly long string in the "organization" property of the control, a crash condition occurs and the Internet Explorer process dies.

2. **Zero Day Vulnerability: Hummingbird HostExplorerTerminal "GetToolbar" Buffer Overflow**

   If an attacker passes an overly long string to the "GetToolbar" method of the control, a crash condition occurs with Internet Explorer.

3. **Zero Day Vulnerability: Hummingbird HostExplorerTerminal "LoadDocfile" Buffer Overflow**

   If an attacker passes an overly long string to the "LoadDocfile" method of the control, a crash condition occurs with Internet Explorer.

4. **Zero Day Vulnerability: Hummingbird PrintExplorerCtrl "SavePrinterProfile" Buffer Overflow**

   If an attacker passes an overly long string to the "SavePrinterProfile" method of the control, a crash condition occurs with Internet Explorer.

5. **Zero Day Vulnerability: Hummingbird PrintExplorerCtrl "Host" Buffer Overflow**

   If an attacker passes an overly long string to the "Host" property of the control, a crash condition occurs with Internet Explorer.

6. **Zero Day Vulnerability: Hummingbird PrintExplorerCtrl "LUName" Buffer Overflow**

   If an attacker passes an overly long string to the "LUName" property of the control, a crash condition occurs with Internet Explorer.

7. **Zero Day Vulnerability: Hummingbird PrintExplorerCtrl "CodeBaseURL"**

   If an attacker passes an overly long string to the "CodeBaseURL" property of the control, a crash condition occurs with Internet Explorer.

   The exploitability of this vulnerability was not determined due to time constraints. The following CVSS score is based on the type and cause of the crash condition, as well as its similarity to other crashes that were demonstrated to be exploitable.

8. **Zero Day Vulnerability: Hummingbird PrintExplorerCtrl "DisplayProfile"**

   If an attacker passes an overly long string to the "DisplayProfile" property of the control, a crash condition occurs with Internet Explorer.

   The exploitability of this vulnerability was not determined due to time constraints. The following CVSS score is based on the type and cause of the crash condition, as well as its similarity to other crashes that were demonstrated to be exploitable.

9. **Zero Day Vulnerability: Hummingbird PrintExplorerCtrl "HTMLFileTitle"**

   If an attacker passes an overly long string to the "HTMLFileTitle" property of the control, a crash condition occurs with Internet Explorer.

   The exploitability of this vulnerability was not determined due to time constraints. The following CVSS score is based on the type and cause of the crash condition, as well as its similarity to other crashes that were demonstrated to be exploitable.

10. **Zero Day Vulnerability: Hummingbird PrintExplorerCtrl "PrinterProfile"**

    If an attacker passes an overly long string to the "PrinterProfile" property of the control, a crash condition occurs with Internet Explorer.

    The exploitability of this vulnerability was not determined due to time constraints. The following CVSS score is based on the type and cause of the crash condition, as well as its similarity to other crashes that were demonstrated to be exploitable.

11. **Zero Day Vulnerability: Hummingbird HCLXWebHostCtrl "PlainTextPassword"**

    If an attacker passes an overly long string to the "PlainTextPassword" property of the control, a crash condition occurs with Internet Explorer.

The exploitability of this vulnerability was not determined due to time constraints. The following CVSS score is based on the type and cause of the crash condition, as well as its similarity to other crashes that were demonstrated to be exploitable.

12. Zero Day Vulnerability: Hummingbird HCLXWebHostCtrl "Src"

If an attacker passes an overly long string to the "Src" property of the control, a crash condition occurs with Internet Explorer.

The exploitability of this vulnerability was not determined due to time constraints. The following CVSS score is based on the type and cause of the crash condition, as well as its similarity to other crashes that were demonstrated to be exploitable.

13. Zero Day Vulnerability: Microsoft WebBrowser "ReadyState"

If an attacker passes an overly long string to the "ReadyState" property of the control, a crash condition occurs with Internet Explorer.

The exploitability of this vulnerability was not determined due to time constraints. The following CVSS score is based on the type and cause of the crash condition, as well as its similarity to other crashes that were demonstrated to be exploitable.

CVSS Baseline Metrics

Access Vector (AV)

The CVSS Access Vector rating is Network (N)—A vulnerability exploitable with network access means the vulnerable software is bound to the network stack, and the attacker does not require local network access or local access. Such a vulnerability is often termed "remotely exploitable." CVSS Rating: AV:N

An attacker can leverage this vulnerable ActiveX control by enticing a user to visit a malicious website in which the control is exploited to gain remote access to their system.

Access Complexity (AC)

The CVSS Access Complexity rating is Medium (M); access conditions are somewhat specialized. CVSS Rating: AC:M

This vulnerability would most commonly require an attacker to perform some amount of social engineering to entice a victim to the malicious Web page with the attack. Additionally, it would be most effectively launched against a victim on whom the attacker has done some information gathering to ensure the presence of the control. The more information gathering performed, the more sophisticated the social engineering could be. When social engineering is not used in the attack, the victim would need to browse to the malicious Web page.

Authentication (Au)

The CVSS Authentication rating is None (N); authentication is not required to access and exploit the vulnerability. CVSS Rating: Au:N

Confidentiality Impact (C)

The CVSS Confidentiality Impact rating is Complete (C); there is a total information disclosure, resulting in all system files being revealed. CVSS Rating: C:C

An attack against this ActiveX control would allow the user full access to the system. The attacker could then take any desired data.

Integrity Impact (I)

The CVSS Integrity Impact rating is Complete (C); there is a total compromise of system integrity. CVSS Rating: I:C

An attack against this ActiveX control would allow the user full access to the system. The attacker could then make any desired changes to the system.

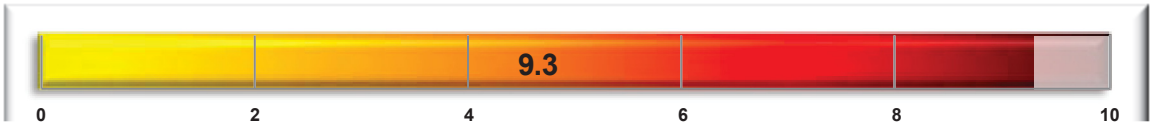
Availability Impact (A)

The CVSS Availability Impact rating is Complete (C); there is a total shutdown of the affected resource. CVSS Rating: A:C

An attack against this ActiveX control would allow the user full access to the system. The attacker could then render the system completely unavailable.

Vulnerability CVSS Score

Table 4. ActiveX vulnerabilities with 9.3 CVSS score.

Scoring Date:	**N/A**	 CVSS Calculator
Base Score	**9.3**	
Impact Subscore	10	
Exploitability Subscore	8.6	
Temporal Score	**Not Defined**	
Overall Score	**9.3**	
		
Vector	(AV:N/AC:M/Au:N/C:C/I:C/A:C)	

ActiveX Vulnerabilities with 4.3 CVSS Score

1. **Zero Day Vulnerability: Hummingbird PrintExplorerCtrl "Connected"**

   If an attacker passes an overly large number to the "Connected" property of the control, a crash condition occurs with Internet Explorer.

2. **Zero Day Vulnerability: Microsoft WebDVDDeviceSegment "AcceptParentalLevelChange"**

   If an attacker passes overly large numbers to the first two parameters of the "AcceptParentalLevelChange" method of the control, a crash condition occurs with Internet Explorer.

3. **Zero Day Vulnerability: Microsoft WebDVDDeviceSegment "StillOff"**

   If an attacker simply calls the "StillOff" method of the control, a crash condition occurs with Internet Explorer.

CVSS Baseline Metrics

Access Vector (AV)

The CVSS Access Vector rating is Network (N)—A vulnerability exploitable with network access means the vulnerable software is bound to the network stack, and the attacker does not require local network access or local access. Such a vulnerability is often termed "remotely exploitable." CVSS Rating: AV:N

An attacker can leverage this vulnerable ActiveX control by enticing a user to visit a malicious website in which the control is exploited to gain remote access to their system.

Access Complexity (AC)

The CVSS Access Complexity rating is Medium (M); access conditions are somewhat specialized. CVSS Rating: AC:M

This vulnerability would most commonly require an attacker to perform some amount of social engineering to entice a victim to the malicious Web page with the attack. Additionally, it would be most effectively launched against a victim on whom the attacker has done some information gathering to ensure the presence of the control. The more information gathering performed, the more sophisticated the social engineering could be. When social engineering is not used in the attack, the victim would need to browse to the malicious Web page.

Authentication (Au)

The CVSS Authentication rating is None (N); authentication is not required to access and exploit the vulnerability. CVSS Rating: Au:N

Confidentiality Impact (C)

The CVSS Confidentiality Impact rating is None (N); there is no impact to the confidentiality of the system. CVSS Rating: C:N

An attack against this ActiveX control would not likely lead to arbitrary code execution. Thus, no impact to the confidentiality of the system would be sustained.

Integrity Impact (I)

The CVSS Integrity Impact rating is None (N); there is no impact to the integrity of the system. CVSS Rating: I:N

An attack against this ActiveX control would not likely lead to arbitrary code execution. Thus, no impact to the integrity of the system would be sustained.

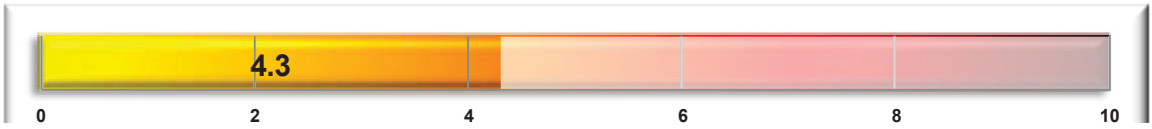
Availability Impact (A)

The CVSS Availability Impact rating is Partial (P); there is reduced performance or interruptions in resource availability. CVSS Rating: A:P

Vulnerability CVSS Score

The exploitability of these vulnerabilities was not determined due to time constraints. This CVSS score is based on the type and cause of the crash condition. This vulnerability is most likely not exploitable and could probably only be used to result in a DoS condition to the Internet Explorer process. However, best practice would be to treat the control as exploitable.

Table 5. ActiveX vulnerabilities with 4.3 CVSS score.

Scoring Date:	**N/A**	 **CVSS Calculator**
Base Score	**4.3**	
Impact Subscore	2.9	
Exploitability Subscore	8.6	
Temporal Score	**Not Defined**	
Overall Score	**4.3**	
		
Vector	(AV:N/AC:M/Au:N/C:N/I:N/A:P)	

Method 1 Mitigations

The best strategy with this vulnerable control is to discontinue use of the component. The easiest and most effective way to stop using the control is to cease using the product that provides the control. If that is not possible then Microsoft has two knowledgebase articles to help facilitate disabling the component:

- Article ID: 240797 - How to stop an ActiveX control from running in Internet Explorer
  - Last Review: August 19, 2011 - Revision: 15.1
  - URL: http://support.microsoft.com/kb/240797
- Article ID: 154036 - How to Disable Active Content in Internet Explorer
  - Last Review: May 10, 2007 - Revision: 4.3
  - URL: http://support.microsoft.com/kb/154036.

If discontinuing the use of the control is not possible, then security updates for the component may be available. This is not as secure as ceasing use of the control as updates may or may not fix the issue. Additionally, assuming updates for the control exist, it will be difficult to test if the issues are mitigated largely because the vulnerability is not publicly disclosed.

Restricting Internet connectivity to the IBM UI Client/Workstation Console can also minimize the vulnerability. An attack would still be possible from any system on the same network as the system; however, this would greater reduce the attack surface of the vulnerability.

Lastly, as malicious links would likely be an element of exploiting this vulnerability, a policy could be established to educate users of the IBM UI Client/Workstation Console to not follow such links, including those received in e-mail, instant messages, Web forums, or Internet relay chat channels.

Method Conclusions

This method focuses on the ActiveX controls installed on the IBM UI Client/Workstation Console (192.168.185.200 – Windows UI). Vulnerable ActiveX controls could allow an attacker to gain control of this part of the system. An attacker can leverage vulnerable ActiveX controls by enticing a user to visit a malicious website in which the control is exploited to gain remote access.

All ActiveX controls on the IBM UI Client/Workstation Console were evaluated for security threats. The IBM UI Client/Workstation Console represents a common installation/configuration used by engineers to interact with the Siemens' Power 3 components. The system contains 3,553 ActiveX controls. Siemens authored four ActiveX controls for use in the ODVWeb area of the system.

The four ActiveX controls authored by Siemens performed very well against the tests and did not cause any crash conditions.

Of the remaining third-party controls, the following vulnerabilities were discovered:

- Total Vulnerable Active X Controls: 5
- Total Vulnerable Methods/Properties (Across 5 Controls): 16
- Proof-of-concept code created for each crash condition
- Exploit code was written for 6 of the 16 vulnerabilities to demonstrate the exploitability of the crashes.

Though it is unlikely that all 16 vulnerabilities identified in this section are exploitable to the point of providing arbitrary code execution, it is recommended that each vulnerability be carefully considered by Siemens to ensure the greatest amount of protection to the IBM UI Client/Workstation Console. This assessment demonstrated that 6 of the 16 are fully exploitable, and lead to arbitrary code execution on the IBM UI Client/Workstation Console, and expect that 13 of the 16 are also exploitable in this way.

5.1.5.2 Method 2: Application Authentication Deep-dive

This method investigates and targets the authentication process used to access the Power 3 applications. A vulnerability exists if authentication to the applications can be bypassed and an attacker is granted un-authenticated access to view and/or update application data.

Vulnerability: Bypass the Power 3 Application Logon Process

A vulnerability exists in the Power 3 application logon process. In the current implementation, the UI server does not perform any client authentication. Instead, the client/server trust relationship relies on the client knowing the public key of the server and generating a token that has been encrypted with this key. Nowhere in the exchange of the token does the server authenticate the client.

CVSS Baseline Metrics

Access Vector (AV)

This vulnerability can be exploited using a standard Web browser configured on a remote host.

The CVSS Access Vector rating is Network (N)—A vulnerability exploitable with network access means the vulnerable software is bound to the network stack, and the attacker does not require local network access or local access. Such a vulnerability is often termed "remotely exploitable." CVSS Rating: AV:N

Access Complexity (AC)

This vulnerability requires understanding the format and processing algorithm of the token used during the logon process of each application. Once the token is understood, implementing code to

generate a valid token is not technically difficult. Given a valid token, exploiting the vulnerability is just a matter of pasting the valid token into the application logon URL in the browser's location bar.

The CVSS Access Complexity rating is Medium (M); access conditions are somewhat specialized. CVSS Rating: AC:M

Authentication (Au)

This vulnerability exists in the logon process to the Siemens applications and allows an attacker access to the applications without having to authenticate.

The CVSS Authentication rating is None (N); authentication is not required to access and exploit the vulnerability. CVSS Rating: Au:N

Confidentiality Impact (C)

This vulnerability provides an attacker access to the Siemens' application data.

The CVSS Confidentiality Impact rating is Partial (P); there is considerable informational disclosure. CVSS Rating: C:P

Integrity Impact (I)

This vulnerability provides the ability for an attacker to update Siemens' application data.

The CVSS Integrity Impact rating is Partial (P); modification of some system files or information is possible. CVSS Rating: I:P

Availability Impact (A)

This vulnerability provides the ability for an attacker to stop system services required by the applications to function.

The CVSS Availability Impact rating is Partial (P); there is reduced performance or interruptions in resource availability. CVSS Rating: A:P

Vulnerability CVSS Score

Table 6. Bypass the Power 3 application logon process CVSS score.

Scoring Date:	**N/A**	 **CVSS Calculator**
Base Score	**6.8**	
Impact Subscore	6.4	
Exploitability Subscore	8.6	
Temporal Score	**Not Defined**	
Overall Score	**6.8**	
		
Vector	(AV:N/AC:M/Au:N/C:P/I:P/A:P)	

Mitigations

The most effective and recommended mitigation for this vulnerability is to authenticate each client that is accessing the Power 3 applications through the Web-based interface. Providing mutual or two-way authentication[9] will ensure no un-trusted or unknown parties are accessing the applications.

Method Conclusions

This method identifies a vulnerability in the token-based logon process used to access the Power 3 applications from the Web-based interface. While the token processing has mechanisms implemented to mitigate a token replay attack, it is possible to generate a valid token outside of the Power 3 architecture that allows un-authenticated access to the applications and the associated data. The vulnerability has a CVSS base score of 6.8.

5.1.5.3 Method 3: Fuzzing

During the discovery process the researcher determined the format of the logon token used to access the Power 3 applications. See Method 2: Application Authentication Deep-dive. With this understanding, the researcher manually fuzzed[10] the key/value pairs that make up the token.

Vulnerability: Logon Token Cross-Site Scripting (XSS)

Constructing a logon token where the username value contained a JavaScript[11] Cross-Site Scripting (XSS)[12] attack, the researcher identified a vulnerability in the processing of the logon token. Using the malicious token to logon to a Power 3 application, the injected JavaScript code is passed through the UI server and executed on the client-side browser. Such an attack is known as a reflected[13] or non-persistent XSS attack.

CVSS Baseline Metrics

Access Vector (AV)

This vulnerability can be exploited using a standard Web browser.

The CVSS Access Vector rating is Network (N)—A vulnerability exploitable with network access means the vulnerable software is bound to the network stack, and the attacker does not require local network access or local access. Such a vulnerability is often termed "remotely exploitable." CVSS Rating: AV:N

Access Complexity (AC)

This vulnerability requires a victim to access a malicious Universal Resource Locator (URL). Additionally, the vulnerability requires understanding the format and processing algorithm of the logon token used during the logon process of Siemens' applications. Once the token is understood, implementing code to generate a valid token is not technically difficult.

The CVSS Access Complexity rating is Medium (M); access conditions are somewhat specialized. CVSS Rating: AC:M

---

9. Mutual authentication http://en.wikipedia.org/wiki/Mutual_authentication, date last accessed November 8, 2011.
10. Fuzzing: Fuzz testing or fuzzing is a black box software testing technique, which basically consists in finding implementation bugs using malformed/semi-malformed data injection in an automated fashion. Ref: The Open Web Application Security Project at http://www.owasp.org/index.php/Fuzzing, date last accessed November 8, 2011.
11. JavaScript http://en.wikipedia.org/wiki/JavaScript, date last accessed November 8, 2011.
12. Cross-Site (XSS) https://www.owasp.org/index.php/Cross-site_Scripting_%28XSS%29, date last accessed November 8, 2011.
13. Reflected XSS https://www.owasp.org/index.php/Cross-site_Scripting_%28XSS%29#Reflected_XSS_Attacks, date last accessed November 8, 2011.

Authentication (Au)

Exploiting the vulnerability requires a Siemens' application logon token, which enables un-authenticated access to the application.

The CVSS Authentication rating is None (N); authentication is not required to access and exploit the vulnerability. CVSS Rating: Au:N

Confidentiality Impact (C)

The CVSS Confidentiality Impact rating is None (N); there is no impact to the confidentiality of the system. CVSS Rating: C:N

Integrity Impact (I)

This vulnerability infects a Web browser with malicious code, but does not infect the entire computer system.

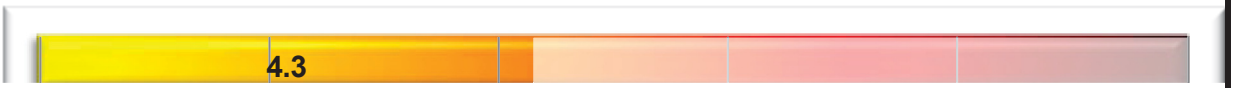
The CVSS Integrity Impact rating is Partial (P); modification of some system files or information is possible. CVSS Rating: I:P

Availability Impact (A)

The CVSS Availability Impact rating is None (N); there is no impact to the availability of the system. CVSS Rating: A:N

Vulnerability CVSS Score

Table 7. Logon token cross-site scripting (XSS) CVSS score.

Scoring Date:	**N/A**	 **CVSS Calculator**
Base Score	**4.3**	
Impact Subscore	2.9	
Exploitability Subscore	8.6	
Temporal Score	**Not Defined**	
Overall Score	**4.3**	
		
Vector	(AV:N/AC:M/Au:N/C:N/I:P/A:N)	

Mitigations

The most effective and recommended mitigation for this vulnerability is to validate the values used in the logon token before use. Even though the generation of the token values is not based on external inputs from the user, secure coding best practices recommend validating all inputs before use.

Method Conclusions

Manual fuzzing of the values used in the key/value pairs of the logon token identified a reflected XSS vulnerability in the logon token processing. The vulnerability has a CVSS score of 4.3.

5.1.5.4 Method 4: Web UI Functionality Evaluation

This method evaluates the Web-based UI and UI server functionality to identify pages and URLs that can be exploited by a malicious user. During the discovery process the researcher identified a URL used to load a file from the UI server file system

A vulnerability exists if the loadfile URL can be exploited to load an arbitrary file from the UI server file system.

Method Conclusions

The researcher verified the loadfile URL does not allow retrieval of arbitrary files from the UI server file system. Testing and examining the process flow of the LoadFileAction class showed the effective use of regular expressions and predetermined paths to mitigate this type of vulnerability when referencing the loadfile URL.

5.1.5.5 Method 5: Session ID Predictability

For stateless protocols such as Hypertext Transfer Protocol (HTTP) and Hypertext Transfer Protocol Secure (HTTPS), Web-based applications and servers maintain a session ID[14] that is used to identify users who have been authenticated. An easily forged or predictable session ID could be exploited to hijack the sessions [15]of legitimate users.

Method Conclusions

The researcher verified the JSESSIONID generated by the ODVWebUI logon process is sufficiently random and is not easily forged or predictable.

5.1.5.6 Method 6: Cross-Site Scripting Attacks

XSS[16] attacks are a special form of code injection, which allows attackers to by-pass client-side security mechanisms. By injecting malicious code into a client, an attacker can gain elevated privileges allowing access to cookies, session tokens, and other sensitive page content. This method checks for XSS vulnerabilities in the Alarm application, specifically the insertion of an alarm comment into the system. An XSS vulnerability exists if a comment containing client-side scripting code can be inserted as a comment, propagated through the system and executed on the Web-based UI.

Method Conclusions

The researcher verified the Alarm comment functionality is not vulnerable to a XSS exploit.

5.1.5.7 Method 7: Privilege Escalation

A privilege escalation[17] attack exploits a vulnerability in a system or application to gain elevated privileges to resources usually protected from the normal end user. Using the WebScarab proxy server, the researcher observed the ODVWebUI/logon.do URL is invoked with HTTP POST method. Examining the arguments being posted to the ODVWebUI logon.do URL, the researcher identified the username variable. During the discovery process the researcher observed that each user is assigned an integer ID. A privilege escalation vulnerability exists if the username variable supplied to the ODVWebUI/logon.do URL can be injected with a different user ID that allows a normal end user to view and/or update protected resources.

---

14. Session ID http://en.wikipedia.org/wiki/Session_ID, date last accessed November 8, 2011.
15. Session hijacking http://en.wikipedia.org/wiki/Session_hijacking, date last accessed November 8, 2011.
16. Cross-Site (XSS) https://www.owasp.org/index.php/Cross-site_Scripting_%28XSS%29, date last accessed November 8, 2011.
17. Privilege Escalation http://en.wikipedia.org/wiki/Privilege_escalation, date last accessed November 8, 2011.

Method Conclusions

The researcher verified that injecting a different username value into the ODVWebUI/logon.do URL did not provide an attack vector for a privilege escalation attack into the UI server or Web-based applications.

5.1.6 Conclusions

All ActiveX controls on the IBM UI Client/Workstation Console were evaluated for security threats. The system contains 3,553 ActiveX controls. Siemens authored four ActiveX controls for use in the ODVWeb area of the system.

The four ActiveX controls authored by Siemens performed very well against the tests and did not cause any crash conditions.

Of the remaining third-party controls, the following vulnerabilities were discovered:

- Total Vulnerable Active X Controls: 5
- Total Vulnerable Methods / Properties (Across 5 Controls): 16
- Proof-of-concept code created for each crash condition
- Exploit code was written for 6 of the 16 vulnerabilities to demonstrate the exploitability of the crashes.

Though it is unlikely that all 16 vulnerabilities identified in this section are exploitable to the point of providing arbitrary code execution, it is recommended that each vulnerability be carefully considered by Siemens to ensure the greatest amount of protection to the IBM UI Client/Workstation Console. This assessment demonstrated that 6 of the 16 are fully exploitable, and lead to arbitrary code execution on the IBM UI Client/Workstation Console, and expect that 13 of the 16 are also exploitable in this way. All of the ActiveX vulnerabilities were in third-party code used by the Siemens system. Siemens will need to work with the third-party vendor in resolving these issues.

The remaining vulnerabilities are related to the Power 3 application logon process and are the result of trusting clients without authentication and of trusting input without proper validation.

5.2 Target 2 – Communications Front-End and Remote Front End Servers

5.2.1 Introduction

The objective of this section of the assessment was to identify any existing vulnerabilities in the CFE/RFE sections of the Power 3 system. While the main target was the communications path with the RTU itself, other programs running on these two systems were also tested. Generally speaking, the choice of programs to test was based on the availability of network access to those programs; either from the inside or outside of the network.

This section attempts to extract the pertinent information from the Cyber Researcher's report on AT2. The Cyber Researcher's report documents to a level where "someone similarly skilled in the art" can reproduce the results. This level is not required for the general report. For the reader that needs this level of detail, read the attached Cyber Researcher's report: AT2 – Communications Front-End and Remote Front-End Servers.

AT2 - Communications Fron

5.2.2 Significance

The RTU communications path is generally unencrypted and frequently crosses into external networks. Compromise of the RTU communications stack would theoretically allow an attacker access to key parts of the Power 3 system from a less-trusted network. Additional programs tested are significant due to the possibility of network access from untrusted users or networks.

5.2.3 Rules of Engagement

All assessment work was done from what would be considered the inside of the Power 3 network. The test system had one RTU set up within those boundaries, which is not necessarily indicative of a Power 3 installation in a production environment. Source code was not made available for any of the services running on the CFE/RFE.

5.2.4 Assessment

For this assessment the majority of the network facing programs on the RFE and CFE systems, along with the RTU communications path, were tested. Focus was given to known weak points in the Distributed Network Protocol (DNP), as well as to programs that could give an attacker access from less-trusted networks.

5.2.4.1 Method 1: Fuzzing

This method was mainly used for testing the RTU communication path. Python was the main tool used for this portion of the assessment. Wireshark was also used to examine communications between the fuzzer and the CFE. The fuzzer used was written completely in Python, and then used to test the DNP functionality within the CFE system. Additionally, IDA Pro was used to disassemble the DNP daemon and related libraries in an attempt to discover their inner workings.

The DNP contains its own fragmentation support, as it was originally used on serial devices. This support can be a source of buffer overflows and other issues, as a client acting as a RTU can send overly large and/or numerous fragments in response to a data request. Several permutations of this particular issue were tested; however, no issues arose with regards to message fragmentation. Additionally, the daemon was resilient to attempts to respond with several different kinds of invalid application data packets, such as invalid point ranges, improperly specified packet types, etc.

Method Conclusions

Known vulnerable points in the DNP were tested; however, the DNP service dealt with improper input accordingly. Attempts were also made to respond with very large amounts of information. Again, the DNP service handled these without failure, and did not consume overly large amounts of resources (other than the requisite network bandwidth to send the information) while processing the response.

5.2.4.2 Method 2: Reverse Engineering

Other programs present on the Power 3 system were analyzed with this method. The program examined on the RFE system was the *RfeMaster* process. Programs examined on the CFE system were the *CfeTestAndDiagnosisAgent*, the *CfeDNP30* daemon (see Method 1), and the *IpcDaemon* process. Additionally, several libraries were examined in the process, covering a wide range of functionality. IDA Pro was used extensively to discover the workings of these programs, as well as the *dbx* debugger present on the IBM AIX operating system.

Some of these processes required encrypted communications to connect, and the assessment team was able to retrieve the required password for the security certificate from one of the libraries used. The program *stunnel* was used along with *netcat* to facilitate encrypted communications and testing once the certificate was decrypted.

Zero Day Vulnerability: RfeMaster Denial of Service

When the *RfeMaster* program (resident on the RFE server) is started, it forks a number of child processes equal to a value set in its configuration file. Each of these processes is bound to a port, and waits for a client connection. The interface for this program is a fairly basic command interpreter, encompassing several simple commands: *Read* and *ReadEx*, *Write* and *WriteEx*, *Configuration*, *Connect*, and *Disconnect*. This particular vulnerability covers an issue that arises with malicious input using the *Read* and *Write* commands.

The program's command interpreter copies memory from the input command into other buffers when it receives data from the Write command. However, all *memcpy* calls are protected by checks to ensure that the data being copied is less than the size of the buffer (4096 bytes), and does not call *memcpy* if it is. However, both the *Read* and *Write* commands return a status message, and this is where the vulnerability resides.

When sending a *Read* command with a sufficiently large *Nbr* argument (above 4095), the program will return garbage output along with the completion message. Sending an overly large *Nbr* argument will cause the program to terminate instantly, due to a segmentation fault in *libssl*'s send functionality. However, if the client sends a command with this large *Nbr* argument then disconnects and reconnects, sending overly large *Nbr* arguments will no longer instantly cause a crash. Instead, the program will begin to consume a large portion of Central Processing Unit (CPU) time and memory, and then finally print out its stack to the client. Afterwards, the program crashes due to a segmentation fault.

This vulnerability allows a client to examine the program stack and cause a DoS condition. Additionally, a client could send invalid data to all of the process's children, causing the aforementioned high CPU and memory usage to notably affect the operation of the RFE server. The test server was configured to have 16 *RfeMaster* child services running, allowing an attacker to consume a large amount of resources with little input from their side.

CVSS Baseline Metrics

Access Vector (AV)

This program binds to the internal network interface of the server. Therefore, access to the local network would be required to exploit it.

The CVSS Access Vector rating is Network (N)—A vulnerability exploitable with network access means the vulnerable software is bound to the network stack, and the attacker does not require local network access or local access. Such a vulnerability is often termed "remotely exploitable." CVSS Rating: AV:N

Access Complexity (AC)

The attack requires access to the encrypted communications that the program uses.

The CVSS Access Complexity rating is Medium (M); access conditions are somewhat specialized. CVSS Rating: AC:M

Authentication (Au)

The affected service does not perform user authentication before allowing access to its command interface.

The CVSS Authentication rating is None (N); authentication is not required to access and exploit the vulnerability. CVSS Rating: Au:N

Confidentiality Impact (C)

Access to the program's stack can impart a reasonably large amount of information about the system.

The CVSS Confidentiality Impact rating is Partial (P); there is a considerable informational disclosure. CVSS Rating: C:P

Integrity Impact (I)

The CVSS Integrity Impact rating is None (N); there is no impact to the integrity of the system. CVSS Rating: I:N

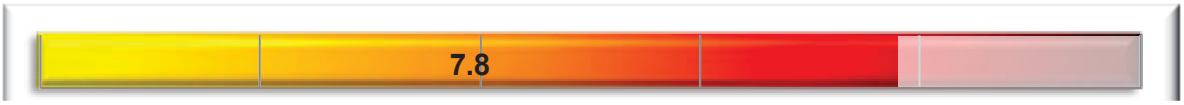
Availability Impact (A)

This vulnerability allows an attacker to completely shut down the service, as well as consume an immense amount of CPU and memory resources.

The CVSS Availability Impact rating is Complete (C); there is a total shutdown of the affected resource. CVSS Rating: A:C

Vulnerability CVSS Score

Table 8. *RfeMaster* DoS CVSS score.

Scoring Date:	**N/A**	 **CVSS Calculator**
Base Score	**7.8**	
Impact Subscore	7.8	
Exploitability Subscore	8.6	
Temporal Score	**Not Defined**	
Overall Score	**7.8**	
		
Vector	(AV:N/AC:M/Au:N/C:P/I:N/A:C)	

Mitigations

The use of encryption ensures that access is restricted. However, any user with access to the Power 3 system can send these invalid commands through other nodes in the system. The fault appears to be within the confirmation function of the program. This function sends completion messages to the client after a command, and appears to read off the end of its buffer if sent an overly large *Read* message. Mitigation should include inspecting and patching the involved code to ensure that it does not read past valid memory.

Concern: Encryption Certificate Retrieval and Decryption

Programs that use encryption on the Power 3 system utilize a Secure Socket Layer (SSL) certificate stored in */home/s/certificates/SP3_Server*, named *SP3_Server-certificate-all.pem*. These certificates are stored with read-only permissions for all groups. These permissions allow for anyone to retrieve the encrypted certificate file, but not decrypt it. Analyzing the *libPcfSsl.so* library showed that an outside program, *getfromsoup,* is used to retrieve the password, and it is stored in a global variable within the library. Permissions to use a debugger would allow a user to access the password, or one could disassemble the library to get the required command line for *getfromsoup*. The program keeps this password resident in memory during its entire life, increasing the chance that an attacker could retrieve it.

Zero-Day Vulnerability: Arbitrary Code Execution with RfeMaster

The *RfeMaster* program (resident on the RFE server) suffers from a vulnerability involving the *Configuration* command. When sent, a specially formed Configuration command the program will reinitialize certain parts of itself, then link its internal function pointers to functions within the library specified by the command. This library could be anywhere on the filesystem, and will have code executed

as long as it exports the symbols expected by the *RfeMaster* program. An attacker would require access to the program's command interface and access to the filesystem to exploit this vulnerability.

CVSS Baseline Metrics

Access Vector (AV)

This program binds to the internal network interface of the server. Therefore, access to the local network would be required to exploit it

The CVSS Access Vector rating is Network (N)—A vulnerability exploitable with network access means the vulnerable software is bound to the network stack, and the attacker does not require local network access or local access. Such a vulnerability is often termed "remotely exploitable." CVSS Rating: AV:N

Access Complexity (AC)

This attack requires access to the encrypted communications that the program uses.

The CVSS Access Complexity rating is Medium (M); access conditions are somewhat specialized. CVSS Rating: AC:M

Authentication (Au)

The CVSS Authentication rating is None (N); authentication is not required to access and exploit the vulnerability. CVSS Rating: Au:N

Confidentiality Impact (C)

This exploit allows an attacker to execute arbitrary code using the *RfeMaster* process.

The CVSS Confidentiality Impact rating is Complete (C); there is a total information disclosure, resulting in all system files being revealed. CVSS Rating: C:C

Integrity Impact (I)

An attacker could modify anything that the process owner could. As the process is owned by *spsy*, an account with high privileges, this encompasses much of the system.

The CVSS Integrity Impact rating is Complete (C); there is a total compromise of system integrity. CVSS Rating: I:C

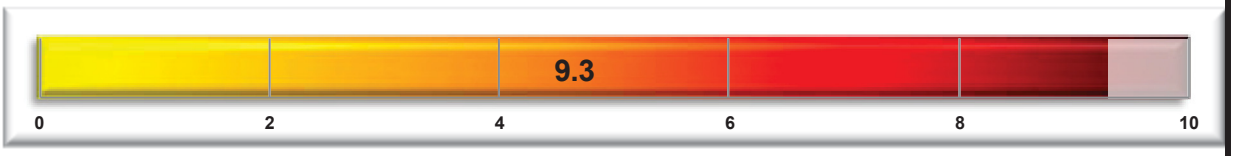
Availability Impact (A)

This vulnerability can easily be used to cause the program to crash by loading malicious code.

The CVSS Availability Impact rating is Complete (C); there is a total shutdown of the affected resource. CVSS Rating: A:C

Vulnerability CVSS Score

Table 9. Arbitrary code execution with RfeMaster CVSS score.

Scoring Date:	**N/A**	 CVSS Calculator
Base Score	**9.3**	
Impact Subscore	10	
Exploitability Subscore	8.6	
Temporal Score	**Not Defined**	
Overall Score	**9.3**	
		
Vector	(AV:N/AC:M/Au:N/C:C/I:C/A:C)	

Mitigations

The best mitigation to this problem would be path validation to ensure that the client cannot redirect execution to a library in an unsecured part of the system (ex: /tmp). Additionally, some form of user authentication would help to ensure that untrusted users cannot access the program's command interpreter.

Zero-Day Vulnerability: Password Database Decryption

The *getfromsoup* program fetches a list of usernames and passwords, along with group information from a database and serializes it to a file. When the *libPcfSsl* library accesses this program to retrieve the certificate password, the program opens the serialized database and decrypts the appropriate username and password. This library uses AES-128 encryption, and the key is stored as a string in the binary. Disassembly of this binary led to discovery of the key, and a simple program was written to decrypt the contents of the database. This database and the program are both readable by world, so any user with access to the system could retrieve them.

CVSS Baseline Metrics

Access Vector (AV)

Local file system access is required, although no special privileges are needed otherwise.

The CVSS Access Vector rating is Local (L) – A vulnerability exploitable with only *local access* requires the attacker to have either physical access to the vulnerable system or a local (shell) account. CVSS Rating: AV:L

Access Complexity (AC)

Access to the system, as well as the ability to reverse engineer parts of the *getfromsoup* binary is required.

The CVSS Access Complexity rating is Medium (M); access conditions are somewhat specialized. CVSS Rating: AC:M

Authentication (Au)

Authentication to the system is required, although no special privileges are needed.

The CVSS Authentication rating is Single (S); one instance of authentication is required to access and exploit the vulnerability. CVSS Rating: Au:S

Confidentiality Impact (C)

This vulnerability gives an attacker access to a wide variety of account information. A large amount of information is likely vulnerable to someone with access to these credentials.

The CVSS Confidentiality Impact rating is Partial (P); there is a considerable informational disclosure. CVSS Rating: C:P

Integrity Impact (I)

An attacker could use the resulting credentials to access or modify some files related to the Power 3 system.

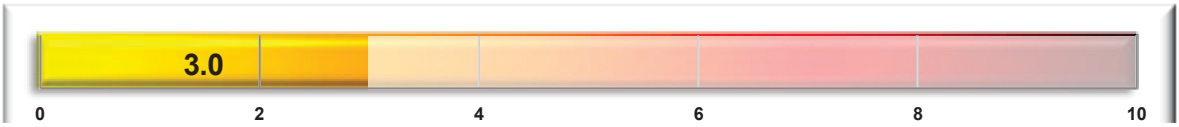
The CVSS Integrity Impact rating is Partial (P); modification of some system files or information is possible. CVSS Rating: I:P

Availability Impact (A)

The CVSS Availability Impact rating is None (N); there is no impact to the availability of the system. CVSS Rating: A:N

Vulnerability CVSS Score

Table 10. Password database decryption CVSS score.

Scoring Date:	**N/A**	 **CVSS Calculator**
Base Score	**3**	
Impact Subscore	4.9	
Exploitability Subscore	2.7	
Temporal Score	**Not Defined**	
Overall Score	**3.0**	
		
Vector	(AV:L/AC:M/Au:S/C:P/I:P/A:N)	

Mitigations

The password databases should not have world readable permissions. Additionally, it is reasonably simple to extract the encryption key from the *getfromsoup* binary, which is also world readable. Removing these permissions would help ensure that less-trusted users would not be able to access these resources.

Method Conclusions

Reverse engineering and testing of these programs lead to some success in encountering vulnerabilities within them. Gaining access to the encrypted communications they use allowed for more extensive testing, as well. The affected services all reside on the RFE server within the Power 3 system. The reported vulnerabilities allow for a combination of DoS attacks, as well as remote code execution on the system.

5.2.5 Assessment Conclusions

The assessment goals were met with a combination of the methods listed above. All accessible services were given some of the available time and effort, especially the RTU communications path. While the DNP is rather complex, this assessment tested the most common points of failure, as well as other possible points based on disassembly and analysis of the DNP service. Overall, the main problems lay with a lack of authentication on the *RfeMaster* service, as well as permissions issues regarding several files/directories on the system.

5.3 Target 3 – Communications Protocol

5.3.1 Introduction

The objective of this section of the assessment was to evaluate the proprietary protocols used by the Power 3 system—specifically, protocols that are used to communicate over IP-based networks.

This section attempts to extract the pertinent information from the Cyber Researcher's report on AT3. The Cyber Researcher's report documents to a level where "someone similarly skilled in the art" can reproduce the results. This level is not required for the general report. For the reader that needs this level of detail, read the attached Cyber Researcher's report: AT3 – Communications Protocol.

AT3 - Communications Proto

5.3.2 Significance

Protocols used for inter-host communication are both a vital means for transferring data between physically separate machines, but also the primary attack vector for remote attacks. Insecure protocols can allow for attacker control of critical processes, or complete control of the system hosts themselves.

5.3.3 Rules of Engagement

Source code was not provided for this assessment. There were no other restrictions.

5.3.4 Assessment

The primary protocol used in the Power 3 system, the Softbus protocol, was thoroughly evaluated during the Phase 1 assessment of the Power 3 Version 3.9 system. As such, it was not particularly focused on in this assessment. Instead, focus was placed on two primary areas: the implementation of SSL layers for Softbus and other protocols used in the system, and plaintext protocols accessible from the network.

In both cases, combinations of reverse engineering (utilizing Ida Pro[18]) and fuzzing were used. Reverse engineering is the process of analyzing the low-level instructions of a program or library to understand its higher-level operational functions and algorithms. Fuzzing is the process of subjecting a

18. IDA Pro disassembler: Ref: http://www.hex-rays.com/idapro/, last accessed November 8, 2011.

target application to generated malformed inputs with the goal of identifying unhandled conditions that can be exploited.

5.3.4.1 Concern: Data Server ("ds") Applications

Each of the data server applications that run on the MM server (192.168.185.107) utilized one of the two OpenSSL implementations above for client authentication. However, one application in particular, *idads*, behaved differently when a connection was made to it from an unauthenticated host. This particular data server application does not appear to correctly implement its SSL handshake, and accepts a single byte from the client into a buffer that then gets read repeatedly.

A message is printed to the system log when a client connects and sends a single byte indicating that a coredump has been avoided. Indeed, no coredump occurs. Researchers were not able to send a byte to the *idads* application that caused any other behavior, although not all 255 possible values were tried as only 1 byte could be sent per instance of *idads*. This meant that the application had to be restarted for each individual test case, which was not possible given time constraints.

It seems unusual that the *idads* application would behave differently from all the other data servers in this regard, and the error message gives an indication that there are likely to be other coding issues within the application.

5.3.4.2 Concern: dsiServer Callback Registration

While reversing the *dsiServer* application, a number of methods were seen dealing with the remote registration of callbacks. A callback is a reference to executable code that is passed as an argument to other code. In this case, it appears that callbacks may be registered remotely, over the network. Researchers registered a number of callbacks, both valid and invalid, but were not able to trigger execution of the callback through testing. It is strongly encouraged that a code audit be performed of the *dsiServer* application code to identify exactly how and where the callbacks are executed, and validate that they cannot be registered or triggered by an unauthenticated remote user.

5.3.4.3 Concern: Signed Integer Comparisons

Throughout the assessment researchers noticed a distinct lack of concern for the sign of integers when performing comparisons. This would not necessarily be a problem if unsigned integers were being used; however, very few unsigned integers were seen. This can lead to severe unintended consequences—especially when dealing with variables representing buffer or message lengths. Unless specifically necessary, signed integers are a poor choice for size fields as they can make performing proper comparisons difficult resulting in damaging buffer overflows. It is recommended that Siemens review and audit their code base for comparisons using signed integers, especially those that are externally influenced.

5.3.4.4 Zero Day Vulnerability: dsiServer Stack-Based Buffer Overflow

There is a stack-based buffer overflow vulnerability in the *dsiServer* process running on the UCS host. Sending a crafted *MS*-type message triggers the vulnerability, which is the result of the application using attacker controlled values for the *count* and *source* arguments for a call to *memmove*. The *memmove* function copies *count* bytes from *source* to *destination* without bounds checking. If the *count* is larger than the size of the destination buffer, an overflow will occur.

CVSS Baseline Metrics

Access Vector (AV)

The CVSS Access Vector rating is Network (N)—A vulnerability exploitable with network access means the vulnerable software is bound to the network stack, and the attacker does not require local

network access or local access. Such a vulnerability is often termed “remotely exploitable.” CVSS Rating: AV:N

The vulnerability does not require local network access to attack. This vulnerability would be an example of the classically defined “remotely exploitable” vulnerability, accessible via routed (i.e., Layer 3 or the Network Layer in the OSI model) networks.

Access Complexity (AC)

The CVSS Access Complexity rating is Medium (M); access conditions are somewhat specialized. CVSS Rating: AC:M

The attacker would need access to the dsiServer application in either binary or source form to test for and develop the attack. Once that is acquired, the discovery and exploitation is relatively simple.

Authentication (Au)

The CVSS Authentication rating is None (N); authentication is not required to access and exploit the vulnerability. CVSS Rating: Au:N

Confidentiality Impact (C)

The CVSS Confidentiality Impact rating is Complete (C); there is a total information disclosure, resulting in all system files being revealed. CVSS Rating: C:C

The attacker is able to read all of the system’s data (memory, files, etc.)

Integrity Impact (I)

The CVSS Integrity Impact rating is Complete (C); there is a total compromise of system integrity. CVSS Rating: I:C

There is a complete loss of system protection, resulting in the entire system being compromised. The attacker is able to modify any files on the target system.

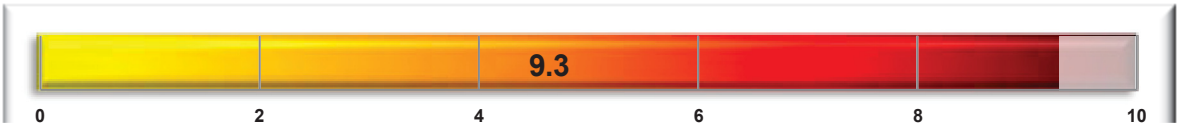
Availability Impact (A)

The CVSS Availability Impact rating is Complete (C); there is a total shutdown of the affected resource. CVSS Rating: A:C

The attacker can render the resource completely unavailable.

Vulnerability CVSS Score

Table 11. *dsiServer* stack-based buffer overflow CVSS score.

Scoring Date:	**N/A**	 **CVSS Calculator**
Base Score	**9.3**	
Impact Subscore	10	
Exploitability Subscore	8.6	
Temporal Score	**Not Defined**	
Overall Score	**9.3**	
		
Vector	(AV:N/AC:M/Au:N/C:C/I:C/A:C)	

Mitigations

The primary mitigation for this vulnerability is to perform proper data validation before use, in accordance with secure coding best practices. Specifically, the data types being used by the application and expected by the methods being called by the application need to be considered when performing data validation.

5.3.5 Conclusions

This assessment target looked at the implementation of the SSL, on which the majority of Power 3 protocols now lay, and found it to be generally well implemented. One concern was identified with a data server application that behaved differently than other data server applications. Servers that did not require authentication were assessed, resulting in an exploitable buffer overflow with a CVSS base score of 9.3. A concern was found with the same process regarding the control it may provide to attackers. A final concern was noted regarding the use of signed integers to represent lengths, which can be difficult to account for when performing comparisons.

5.4 Target 4 – Communicator Server

5.4.1 Introduction

The Realtime COM server is the main data distribution server within the Power 3 system. The data is retrieved from the field devices by the CFE and RFE servers or received from other control centers by the UCS and is passed to the COM for processing. The processed data, alarms, and messages are then sent to the UI, Application software, and HIS.

This section attempts to extract the pertinent information from the Cyber Researcher's report on AT4. The Cyber Researcher's report documents to a level where "someone similarly skilled in the art" can reproduce the results. This level is not required for the general report. For the reader that needs this level of detail, read the attached Cyber Researcher's report: AT4 – Communications Server.


AT4 - Communicator Server.pdf

5.4.2 Objective

The objective of this section of the assessment was to identify any vulnerability in the COM Data Server. Process data for the SCADA system is stored in the data base on the COM server along with the current switching statuses; another key part of the operations of the COM is the dynamic master block function for the process data base files, which run on the COM.

5.4.3 Significance

The COM server is the center of SCADA data and command processing and distribution. The Basic Data Processing (BDP) function block runs in the COM and communicates with most of the other servers in the system. BDP functions include:

- Status change processing
- Limit processing
- Extrema processing (minimums, maximums)
- Calculation processing
- Integration processing
- Abnormal processing
- Storage in Network Image (NIM) database
- Generation of alarms
- Update of world maps (one-line displays) with current data
- Notification of other applications (programs) of the new data
- Maintain signalization data.[19]

5.4.4 Rules of Engagement

There were no rules of engagement that impacted this portion of the assessment. Source code was not provided for this assessment.

The system under test did not include typical perimeter connections to attack from (i.e., a corporate network and firewall, Demilitarized Zone [DMZ], vendor connection, modem pool, or Intercontrol Center Communication Protocol [ICCP] connection) since the focus of the assessment project was to determine the cyber security posture of the core system hardware and software configuration. Therefore, the assessment was conducted from INL computers connected directly to the Power 3 EMS/SCADA and RTU communications network.

5.4.5 Assessment

This assessment looked for ways to disrupt COM functionality or corrupt the data it distributes.

The open ports and services available on the COM host are listed in Table 12 below. These services were the focus of this assessment because they are exposed to the network.

19. Siemens Energy, Inc., *Spectrum Power 3 SCADA Software Details: Basic Data Processing*,Dec 2008, p. 3.

Table 12. Ports and services available on the COM.

Port	Service
22/tcp	OpenSSH 5.4 (protocol 2.0)
111/tcp/udp	portmapper
2049/tcp/udp	NFS
9711/tcp	BULS

5.4.5.1 Method 1: NFS

The Spectrum Power 3.9 assessment reported that the AIX servers export directories via Network File System (NFS). This was validated to be true of the 3.10 system as well. See the *AT7: Validation of Previous INL Assessment Results for Spectrum Power 3 Release 3.9 Cyber Research Report* for more details.

Configuration-Induced Vulnerability: Power 3 files accessible via NFS

An attacker is able to spoof a trusted IP address and mount the COM's /home directory.

A successful attack via the NFS exports would nullify all security mechanisms the Power 3 system uses to prevent unauthorized access and control to untrusted entities. Regardless of its CVSS Score, this issue should be considered highly significant.

CVSS Baseline Metrics

Access Vector (AV)

The CVSS Access Vector rating is Adjacent Network (A) – A vulnerability exploitable with *adjacent network access* requires the attacker to have access to either the broadcast or collision domain of the vulnerable software. CVSS Rating: AV:A

Access Complexity (AC)

The CVSS Access Complexity rating is Low (L); specialized access conditions or extenuating circumstances do not exist. CVSS Rating: AC:L

Authentication (Au)

The CVSS Authentication rating is None (N); authentication is not required to access and exploit the vulnerability. CVSS Rating: Au:N

Confidentiality Impact (C)

The CVSS Confidentiality Impact rating is Partial (P); there is considerable informational disclosure. CVSS Rating: C:P

Even though the entire host file system is not exposed, the part of the file system that is exposed encompasses the entire SCADA system.

Integrity Impact (I)

The CVSS Integrity Impact rating is Partial (P); modification of some system files or information is possible. CVSS Rating: I:P

Even though the integrity of the entire host file system is not at risk, the part of the file system that can be modified encompasses the entire SCADA system.

Availability Impact (A)

The CVSS Availability Impact rating is Complete (C); there is a total shutdown of the affected resource. CVSS Rating: A:C

An attacker an overwrite files that are necessary for system operation.

Vulnerability CVSS Score

Table 13. Power 3 files accessible via NFS CVSS score.

Scoring Date:	**N/A**	 **CVSS Calculator**
Base Score	**7.3**	
Impact Subscore	8.5	
Exploitability Subscore	6.5	
Temporal Score	**Not Defined**	
Overall Score	**7.3**	
		
Vector	(AV:A/AC:L/Au:N/C:P/I:P/A:C)	

Mitigations

The recommended mitigations for the vulnerability are as follows: do not export directories that do not need to be exported; prevent access to NFS server ports on all hosts that do not need to export directories; and tunnel NFS over Secure Shell (SSH) or upgrade to NFS Version 4 and configure the system to use its authentication and encryption security options.

Concern: AIX passwords are truncated to 8 characters

While performing assessment activities, the assessment team discovered that the AIX passwords are truncated to eight characters. This means that an attacker only needs to guess (or crack) the first eight characters of the AIX account passwords. For example, the root password was documented as Sp3ctr^m310, but only Sp3ctr^m is required to log in as root.

Mitigations

The default AIX configuration truncates passwords to eight characters. Instructions for configuring AIX to allow longer passwords can be found at the following site:

https://www-304.ibm.com/support/docview.wss?uid=isg3T1010741

Method Conclusions

The integrity, availability, and confidentiality of all Power 3 files exported via NFS are at risk. The NFS implementation on the 3.10 system still only utilizes IP and user ID-based authentication, which can be circumvented.

SSH private keys and the certificates used for SSL authentication are located on NFS exports. Private keys and certificates should be well protected. In the current configuration, they can be copied by anyone able to NFS mount the /home directory. The private keys are not encrypted and can be used to authenticate to the Power 3 hosts without a password. The SSL certificates are encrypted with a password, which was cracked by the assessment team, and is also available in binaries that are shared and accessible via the NFS exports.

The Softbus security preferences configuration file can be edited via NFS. It is possible to change the Softbus security options that set the security modes these servers will support in the buls.conf file via NFS. This method was used by the assessment team to downgrade Softbus communications to and from the COM server from encrypted to plaintext. From there, no authentication or encryption would be necessary for an attacker to communicate directly with the SCADA system via the Softbus protocol.

The directories exported via NFS should be limited to those necessary for system operation. NFS should be either tunneled over SSH or configured to use NFS Version 4 and its authentication and encryption security options.

5.4.5.2 Method 2: Fuzz Softbus Network Traffic

Power 3 programs communicate exclusively via the Softbus protocol. The BULS application handles all inter-computer communication. Phase 1testing proved the ability to alter Softbus messages sent over the network, such as point values, alarms, and control messages.

This portion of the assessment aimed to identify vulnerabilities in the COM applications that process data from Softbus messages that were sent over the network. The goal was to fuzz[20] the application layer of the Softbus messages.

A Softbus decoder was written that could take intercepted Softbus traffic and provide the details of all passed messages. This data could then be stored for later use or manipulated and passed along to the correct endpoint. The assessment team used traffic captures, Power 3 documentation, and header files to assist in interpreting the data portion of the Softbus messages.

Method Conclusions

This portion of the assessment aimed to identify input validation vulnerabilities in Power 3 applications that process data from Softbus messages.

The assessment team was able to perform some fuzzing of the COM Softbus messages, but did not detect any application crashes. Future Power 3 security assessments should perform further testing for input validation vulnerabilities in the Softbus application layer as well as the other layers of the Softbus protocol stack.

5.4.6 Conclusions

The objective of this assessment target was to assess the COM server for vulnerabilities that may allow unauthorized access to the COM server or disrupt the Power 3 system.

The NFS configuration on the COM server puts the integrity, availability, and confidentiality of all exported Power 3 files at risk. For example, SSH private keys and SSL certificates can be stolen and the BULS security configuration can be edited by an attacker with local network access.

SSH private keys and the certificates used for SSL authentication are located on NFS exports. Private keys and certificates should be well protected. In the current configuration, they can be copied by anyone able to NFS mount the /home directory. The private keys are not encrypted and can be used to

---

20. Fuzzing: Fuzz testing or fuzzing is a black box software testing technique, which basically consists in finding implementation bugs using malformed/semi-malformed data injection in an automated fashion. Ref: The Open Web Application Security Project at http://www.owasp.org/index.php/Fuzzing, date last accessed November 8, 2011.

authenticate to the Power 3 hosts without a password. The SSL certificates are encrypted with a password that was cracked by the assessment team.

The Softbus security preferences configuration file is available for editing via NFS. It is possible to change the Softbus security options that set the security modes these servers will support in the buls.conf file via NFS. This method was used by the assessment team to downgrade Softbus communications to and from the COM server from encrypted to plaintext.

The directories exported via NFS should be limited to those necessary for system operation. NFS should be either tunneled over SSH or configured to use NFS Version 4 and its authentication and encryption security options.

It is necessary to emphasize that a successful attack on the NFS exports would essentially render useless all other protections the Power 3 system provides. Used in combination with any other vulnerability identified in this assessment, or even on its own, the lack of NFS authentication provides an attacker unfettered access and control of any Power 3 host.

Power 3 programs communicate exclusively via the Softbus protocol. The BULS application handles all inter-computer communication. The previous assessment proved the ability to alter Softbus messages sent over the network, such as point values, alarms, and control messages. Phase 1 testing found vulnerabilities in the first two layers of the Softbus network protocol. This assessment performed limited fuzzing on the Softbus application layer to identify input validation vulnerabilities in the COM applications that process data from applications on other Power 3 hosts. Future Power 3 security assessments should perform further testing for vulnerabilities in all three layers of the Softbus protocol stack.

5.5 Target 5 – Applications that Access Oracle

5.5.1 Introduction

The objective of this section of the assessment was to identify any vulnerability in the Power 3 system on processes that accesses the Oracle Database. All Power 3 apps access the ADM static configuration Oracle Database. Certificate authority and the HIS Oracle database resides on the ADM server sections of the Power 3 system and could be vulnerable to escalation of privileges, SQL injection attacks, etc.

This section attempts to extract the pertinent information from the Cyber Researcher's report on AT5. The Cyber Researcher's report documents to a level where "someone similarly skilled in the art" can reproduce the results. This level is not required for the general report. For the reader that needs this level of detail, read the attached Cyber Researcher's report: AT5 – Applications that Access Oracle.

AT5 - Applications that Access Oracle.pd

5.5.2 Significance

If an attacker can exercise influence on the Oracle Database in the Power 3 system, they could steal information, alter data, and disrupt services to all applications in the system with which Oracle communicates, such as the Transmission Network Apps (TNA), HIS, Switching Procedure Management (SPM), and Primitive Data Manager (PDM) systems and programs. This type of attack could lead to the loss of money, time, and reputation in the marketplace. In some specialized instances, it could also have national security implications depending on the attacker and victim.

5.5.3 Rules of Engagement

The SPM module was assessed with regards to its interaction with Oracle, as the database schema, among other things, was missing. However, this assessment investigated Oracle Forms, chief among tools used to interact and configure the SPM. No other restrictions were placed on this assessment target.

5.5.4 Assessment

Various methods were used to identify all the components relevant to the Oracle database on the Power 3 system. Some time was spent using the system, observing communication paths and interactions between components and working with Siemens developers and integrators to gain an understanding of its functionality with relation to Oracle. The following major components of the Power 3 system are acknowledged as performing meaningful interactions with Oracle database:

- TNA: Transmission Network Apps
- HIS: Historical Information System
- SPM: Switching Procedure Management
- PDM: Primitive Data Manager.

Communication paths, tools, scripts, and any other aspect of the system that interacts with Oracle were evaluated for vulnerabilities that would allow an attacker to exercise influence over the database.

5.5.4.1 Method: Oracle Default Accounts Audit

This method audits the usernames and passwords used on the Power 3 system to determine if any accounts are using default credential combinations. Oracle is very well-known to have several default usernames and passwords. Usernames and passwords are often the first line of defense an attacker may try to compromise. This type of comprise would lead to unauthorized authentication to the system.

With the introduction of 10g (the version used in the Power 3 system), the situation has improved significantly. While it is not typically common to find the SYS and SYSTEM account with default passwords, Oracle contains several other accounts that are often neglected. An example of such an account is the DBSNMP (the Intelligent Agent) account. To correctly configure this account, the password must be changed in two places if the account is to remain operational. CTXSYS and MDSYS are other accounts that are frequently abused to gain access to the Oracle system. Another common mistake is when Oracle users restore default usernames and passwords to default settings in support of legacy products with hardcoded passwords.

Method Conclusions

No problems were discovered with the username and password combinations in the Power 3 system.

5.5.4.2 Method: SQL Injection through Web Forms – TNA (Transmission Network Apps) / HIS (Historical Information System) – ODVWeb User Interface

The ODVWeb UI is one of the primary areas in which an attacker could possibly influence, change, and otherwise affect Oracle data in the system. The ODVWeb UI is located on the IBM UI Client/Workstation Console (192.168.185.200). One can log into the ODVWeb UI by clicking the icon on the desktop of the IBM UI Client/Workstation Console.

The sections in the ODVWeb UI that interact with Oracle are concentrated in the TNA and HIS sections. In an attempt to discover potential issues that could lead to an attack from these sections, the assessment team provided specialized data to all the input fields in the TNA and HIS sections.

Concern: Information Disclosure

In some circumstances when invalid data is used in the ODVWeb UI it displays an Oracle message in its bottom window panel. An attacker could easily perceive or discover the error originates from Oracle due to the “ORA-XXXXX” format displayed in the message. This information could aid an attacker in discovering injection points against the database. Additionally, if the ORA-XXXXX portion of the string were missing, an attacker could still search the Internet with the exact error message string to learn the message originates from Oracle.

Mitigations

It would be considered best practice to have the UI process the error message and sanitize the output before displaying it to the user. For example, a sanitization process could remove revealing formats such as the ORA-XXXXX string and reword the message so that an attacker cannot leverage the information to make attack discovery easier. Sanitizing the message makes it more difficult for an attacker to learn the underlying structure of the system and what is and is not working against it.

Method Conclusions

A minor information disclosure issue was discovered during tests against the ODVWeb UI. This issue can be easily remedied by adding a layer of sanitization to the output message to obfuscate its point of origin. No other problems were discovered with the input fields in the TNA and HIS sections.

5.5.4.3 Method: TNA/HIS – ODVWeb User Interface Oracle Communication Deep Dive

In the previous method, this assessment evaluated the ODVWeb UI as one of the primary areas in which an attacker could possibly influence, change, and otherwise affect Oracle data in the system. The ODVWeb UI is located on the IBM UI Client/Workstation Console (192.168.185.200). The ODVWeb UI has the following communication path for its interactions:

IBM UI Client/Workstation Console (192.168.185.200) -> MMI Server (192.168.185.107) -> Intermediate Server(s) -> ADM (192.168.185.101) / Oracle Database.

The IBM UI Client/Workstation Console makes a web request over SSL to the Man-Machine Interface (MMI) server for a Java class to process the request. The Java class processes the request and uses its Java Database Connectivity (JDBC) module to interact with Oracle.

Method Conclusions

No issues in the code that allow SQL Injection possibilities were discovered. The use of parameterized statements was observed and best practices followed to prevent SQL injections in the code.

5.5.4.4 Method: Local Server SQL Injection - TNA/PDM Server Scripts

A key area in which the TNA portion of the system interacts with Oracle is in the server scripts located on the TNA server (192.168.185.103).

When the TNA server starts up it calls a script at /home/s/MCS_CONF/INITSOS. The following call chain is then established by INITSOS:

- The INITSOS script calls /home/s/MCS_CONF/IGNITE_SCRIPTS
  - The IGNITE_SCRIPTS starts a daemon in /home/s/sys/wf_daemon.plx
    - The wf_daemon.plx daemon calls /home/s/sys/na/NaExecSc.plx

The NaExecSc.plx calls several perl scripts located in /home/s/sys/ and /home/s/sys/na/

The scripts located in /home/s/sys/ and /home/s/sys/na/ are responsible for monitoring the Oracle database and reacting to different changes it perceives in the data. As data changes it will react and perform read and write operations to the database. Consequently, a code audit for SQL Injection possibilities was done on those two directories of scripts.

Another area of the system that interacts with Oracle is the PDM. The PDM performs many of its interactions with the Oracle database in scripts located on the ADM server (192.168.185.101) in the directory /home/s/sys/rdbms/. This directory was also audited for SQL Injection possibilities.

SQL Injection is a popular method for attacking databases. This method attacks user-supplied input to an application that directly embeds a dynamic SQL query in its communications with the database.

Because the dynamic query comes from the user supplied input, it is possible for that user to manipulate the query in such a way that additional SQL is executed.

Vulnerability: SQL Injection

There exist a number of host-based SQL Injection vulnerabilities on the TNA and ADM servers. They are listed as host-based as the security researchers did not identify remote paths to exploit the SQL Injection, meaning an attacker would have to have local access to successfully exploit the vulnerability. It should not be assumed that there is not a method to reach these vulnerabilities remotely, as the research team had limited time to investigate the exploitability and may have missed avenues of attack.

SQL Injection is a code injection attack that occurs at the database level of an application. It is one of the most commonly exploited vulnerabilities. SQL injections occur when a user or attacker supplies control characters (double quotes, semi-colons, etc.) as part of a string that is then used to build a query for a database. The control characters, if not properly escaped by the application, can alter the query to the point of allowing anything from information disclosure to arbitrary code execution. The number in the code samples below represents the line number on which the code is found.

CVSS Baseline Metrics

Access Vector (AV)

The CVSS Access Vector rating is Local (L) – A vulnerability exploitable with only *local access* requires the attacker to have either physical access to the vulnerable system or a local (shell) account. CVSS Rating: AV:L

The scripts in question cannot be called or used by communicating with a listening service. It is possible that an attacker could influence some of these scripts to read and write data from an access vector outside of local access if they could control database data by a different mechanism. Such a circumstance is highly specialized and more difficult for an attacker to gain. Thus, the most appropriate rating for this vulnerability is local access.

Access Complexity (AC)

The CVSS Access Complexity rating is Medium (M); access conditions are somewhat specialized. CVSS Rating: AC:M

The user must be the “spsy” user or belong to the “spec” group to call the scripts in question.

Authentication (Au)

The CVSS Authentication rating is None (N); authentication is not required to access and exploit the vulnerability. CVSS Rating: Au:N

If a user can run the scripts no additional authentication is needed.

Confidentiality Impact (C)

The CVSS Confidentiality Impact rating is Complete (C); there is a total information disclosure, resulting in all system files being revealed. CVSS Rating: C:C

A SQL Injection attack would allow a user to gain access to a considerable amount of data in the Oracle database. An attacker can also utilize Oracle functionality to access files outside of the database, making the entire system vulnerable.

Integrity Impact (I)

The CVSS Integrity Impact rating is Complete (C); there is a total compromise of system integrity. CVSS Rating: I:C

A SQL Injection attack would allow a user to manipulate a considerable amount of data in the Oracle database. An attacker can also utilize Oracle functionality to access files outside of the database, making the entire system open.

Availability Impact (A)

The CVSS Availability Impact rating is Complete (C); there is a total shutdown of the affected resource. CVSS Rating: A:C

A SQL Injection attack would allow a user to impact the availability of the Oracle service as well as adversely impacting Power 3 services dependent on the Oracle data. An attacker can also utilize Oracle functionality to access files outside of the database, making the entire system susceptible to DoS attack.

Vulnerability CVSS Score

Table 14. SQL Injection CVSS score.

Scoring Date:	**N/A**	 **CVSS Calculator**
Base Score	**6.9**	
Impact Subscore	10	
Exploitability Subscore	3.4	
Temporal Score	**Not Defined**	
Overall Score	**6.9**	
		
Vector	(AV:L/AC:M/Au:N/C:C/I:C/A:C)	

Mitigations

Perl's DBI, available on the CPAN, supports parameterized SQL calls. Both the do method and prepare method support parameters ("placeholders," as they call them) for most database drivers. However, parameterization cannot be used for identifiers (table names, column names); DBI's quote_identifier() method should be used for identifiers. Writing SQL by hand could also be avoided by using DBIx::Class, SQL::Abstract, etc., to generate SQL programmatically.[21]

It is clear after looking at the server scripts in these areas that some scripts implement best practices to prevent SQL Injection. This practice is observed in scripts such as wf_daemon.plx, wf_run_proc.plx, wf.plx on the TNA server and in the Fill_C_AOR.plx and EAGwConfig.plx on the ADM server. It is recommended that this best practice is universally adopted for all of the server scripts and that outside influence over the SQL queries in the scripts is limited where possible.

21. http://bobby-tables.com/perl.html, last accessed November 8, 2011.

Concern: SQL Execute / Commit on Data from Oracle

While auditing the server scripts for SQL Injection, it was observed that many of the server scripts on the TNA server (192.168.185.103) in the /home/s/sys/ and /home/s/sys/na/ directories query the database for information and then execute subsequent SQL queries based on those results. One example is in the NaSaveXMLConfiguration.plx:

NaSaveXMLConfiguration.plx

- **99:**`insert into xml_directive values(xml_seq_dirno.nextval,'$dirname','$rt','$se','$pa','$ns','$sa','$sd','$vs','$pf','$pe','$va','$at','$fc')`
  - **97:** Most of the values on line 99 come directly from a previous SQL query.

The series of wf____.plx scripts in the /home/s/sys/ directory seem to also pull data from tables in the database on which commands are executed. If an attacker was able to gain control of the data points in these areas of the system, the attacker could leverage these scripts to inject different queries from the database.

Mitigations

Some validations checks should be performed on the data from Oracle on which commands are executed to ensure the data is what the developers expect.

5.5.4.5 Method: PDM /SPM – Oracle Forms

Oracle Forms allows users to interact with the PDM and SPM areas of the system. Oracle Forms was audited for areas in its forms that would allow attacks against the underlying database.

In an attempt to discover potential issues that could lead to an attack from these sections, the assessment team provided specialized data to the input fields. These inputs included, but were not limited to:

- Specialized strings of various lengths, formats, and containing special characters to trigger specific conditions within Oracle
- Numbers of various sizes and formats also specifically crafted for Oracle.

No issue was discovered in Oracle Forms that would allow an attack from these areas.

Method Conclusions

A code audit for SQL Injection in the server scripts located on the TNA server and ADM server reveals that some portions of code allow user input to influence the queries to the database. Because the dynamic query comes from user supplied input, it is possible for a user to manipulate the query in such a way that additional SQL is executed.

It is clear after looking at the server scripts in these areas that some scripts implement best practices to prevent SQL Injection. This practice is observed in scripts such as wf_daemon.plx, wf_run_proc.plx, wf.plx on the TNA server and in the Fill_C_AOR.plx and EAGwConfig.plx on the ADM server. It is recommended that best practices are universally adopted for all of the server scripts and that outside influence over the SQL queries in the scripts is limited where possible.

While auditing the server scripts for SQL Injection, it was observed that many of the server scripts on the TNA server (192.168.185.103) query the database for information and then execute subsequent SQL queries based on those results. This could allow an attacker to inject different queries on the database if the attacker was able to gain control of the data points in these areas of the system. It is recommended that

some validations checks should be performed on the data from Oracle on which commands are performed to try to prevent this type of attack. No issues were found in the Oracle Forms application.

*5.5.4.6 Method: HIS – Pro*C Code*

It was discovered that the HIS uses Pro*C[22] code on the COM server (192.168.185.102) to perform communications with Oracle. As source code was not provided, the assessment team evaluated the binaries located in the /home/s/sys/ directory on the COM server for vulnerabilities associated with Pro*C-based Oracle queries.

Method Conclusions

No problems were discovered with the Pro*C binaries located on the COM server in the /home/s/sys/ directory. This does not imply the absence of exploitable bugs in these binaries, only that none were identified during this assessment.

5.5.5 Conclusions

Various methods were used to identify all the components relevant to the Oracle database on the Power 3 system. The following major components of the Power 3 system are acknowledged as performing meaningful interactions with Oracle database:

- Transmission Network Apps (TNA)
- Historical Information System (HIS)
- Switching Procedure Management (SPM)
- Primitive Data Manager (PDM).

Communication paths, tools, scripts, and any other form of the system that interacts with Oracle were evaluated for vulnerabilities that would allow an attacker to exercise influence over the database.

The usernames and passwords used on the Power 3 system were audited to determine if any accounts are using default credential combinations from Oracle. No problems were discovered in the audit.

The TNA and HIS components are used from the ODVWeb UI on the IBM UI Client/Workstation Console. The assessment team tested the input fields with specialized data in attempt to discover potential issues that could lead to an attack from the ODVWeb UI. A minor information disclosure issue was discovered during the tests. This issue can be easily remedied by adding a layer of sanitization to the output message to obfuscate its point of origin. No other problems were discovered with the input fields.

The assessment team also evaluated the database communications path from the ODVWeb UI to the JDBC module and subsequently to Oracle to determine if any attacks were possible from this area. No issues in the code were discovered. The use of parameterized statements was observed and best practices followed to prevent attacks in this area.

Server scripts belonging to the TNA and the PDM were also audited for attack possibilities. Some server scripts in these areas implement best practices in the code to prevent attacks. However, other scripts do not. It is recommended that best practices are universally adopted for all of the server scripts and that outside influence over the SQL queries in the scripts is limited where possible to prevent attacks leveraging these scripts. Additionally, while auditing the server scripts, it was observed that some scripts query the database for information and then execute subsequent SQL queries based on those results. This could allow an attacker to inject different queries on the database if the attacker was able to gain control of the data points in these areas of the system. It is recommended that validations checks be performed on

22. Pro*C is an embedded SQL programming language used by Oracle. It uses either C or C++ as its base language.

the data from Oracle on which commands are performed to ensure that the data is what the developers expect and prevent attacks.

Pro*C Binaries that interact with the HIS were also evaluated for potential issues and no issues were discovered. Lastly, Oracle Forms was audited due to its association with the PDM and SPM areas of the system. No issues in the forms were discovered that would allow attacks from this area.

5.6 Target 6 – Utility Communications Server

5.6.1 Introduction

This assessment target focuses on the UCS of Power 3 system. The UCS consists primarily of an ICCP server that interfaces with external utilities. The ICCP portion of the UCS was the main subject of testing for this target. Other processes on the UCS were investigated and reported on as part of Assessment Target 3 (AT3).

This section attempts to extract the pertinent information from the Cyber Researcher's report on AT6. The Cyber Researcher's report documents to a level where "someone similarly skilled in the art" can reproduce the results. This level is not required for the general report. For the reader that needs this level of detail, read the attached Cyber Researcher's report: AT6 – Utility Communications Server.

AT6 - Utility Communications Serv

5.6.2 Objective

The objective of this section of the assessment was to identify any vulnerability in the Power 3 system on the UCS. The main focus on the UCS was the implementation of the ICCP and related communications between applications on the system.

5.6.3 Significance

The UCS frequently provides a gateway from internal trusted networks to external untrusted networks through its ICCP application stack. Because of this fact, vulnerabilities in the UCS that are remotely reachable can provide an attacker with a significant foothold into sensitive internal networks. The UCS is also more likely to have externally exposed interfaces, meaning it is more likely to come under attack than other hosts in the Power 3 system.

5.6.4 Rules of Engagement

Siemens did not provide source code for this assessment. As a result, stack-traces are used to communicate the location of vulnerabilities. There were no other restrictions on the assessment.

5.6.5 Assessment

This assessment target focused on the ICCP stack provided by the UCS, to include the third-party Systems Integration Specialists Company, Inc. (SISCO) Open System Interconnection (OSI) networking stack, and Application Programming Interface (API) layer applications.

5.6.5.1 Method 1: ICCP Fuzzing

Fuzzing is an effective method for assessing processes where there is either very little information or an overwhelming amount of information regarding how the process deals with the input streams being manipulated. The actual term "fuzzing" refers to the process of providing malformed inputs to the program under test with the ultimate goal of identifying unhandled errors or other bugs that can lead to exploitable conditions.

The ICCP stack is notably complex, consisting of multiple, frequently redundant layers. The protocol specification itself is complex and requires a large amount of functionality that is not used by the protocol in practice. This leads to an environment ripe for bugs and vulnerabilities that fuzzing is uniquely suited for discovering.

An internally developed ICCP fuzzing application was utilized for testing the ICCP stack of the UCS. The fuzzing application is capable of acting as either a client or server, and can also behave legitimately in a limited fashion.

Vulnerability: SISCO OSI Stack TPKT Layer DoS

There is a null pointer dereference DoS vulnerability in the TPKT layer of SISCO's OSI networking stack for ICCP on the UCS host *uc1inl*. The vulnerability itself is similar to the one identified in CVE-2005-4812, although this crash occurs on an AIX host and not a Windows host.

CVSS Baseline Metrics

Access Vector (AV)

The vulnerable ICCP process on the UCS is remotely reachable over the network.

The CVSS Access Vector rating is Network (N)—A vulnerability exploitable with network access means the vulnerable software is bound to the network stack, and the attacker does not require local network access or local access. Such a vulnerability is often termed "remotely exploitable." CVSS Rating: AV:N

Access Complexity (AC)

The vulnerability can be exploited with a minimal of effort, requiring only network access to the vulnerable host and the ability to send a crafted 4-byte packet.

The CVSS Access Complexity rating is Low (L); specialized access conditions or extenuating circumstances do not exist. CVSS Rating: AC:L

Authentication (Au)

The CVSS Authentication rating is None (N); authentication is not required to access and exploit the vulnerability. CVSS Rating: Au:N

Confidentiality Impact (C)

The CVSS Confidentiality Impact rating is None (N); there is no impact to the confidentiality of the system. CVSS Rating: C:N

Integrity Impact (I)

The CVSS Integrity Impact rating is None (N); there is no impact to the integrity of the system. CVSS Rating: I:N

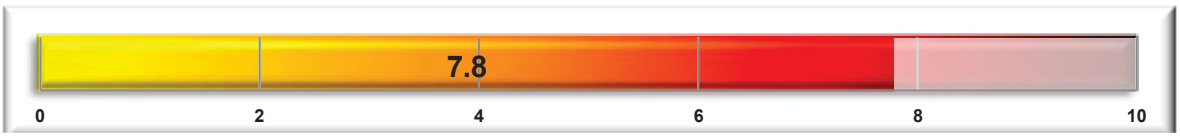
Availability Impact (A)

The CVSS Availability Impact rating is Complete (C); there is a total shutdown of the affected resource. CVSS Rating: A:C

The attacker can render the resource unavailable until a manual restart can be performed.

Vulnerability CVSS Score

Table 15. SISCO OSI stack TPKT layer DoS CVSS score.

Scoring Date:	**N/A**	 **CVSS Calculator**
Base Score	**7.8**	
Impact Subscore	6.9	
Exploitability Subscore	10	
Temporal Score	**Not Defined**	
Overall Score	**7.8**	
		
Vector	(AV:N/AC:L/Au:N/C:N/I:N/A:C)	

Mitigations

It is possible that this crash is in fact the same bug detailed in CVE-2005-4812. In that case, mitigation is a simple process of updating the SISCO OSI stack to the current, patched version. If it is a separate issue, and updating the OSI stack does not fix the problem, then a bug report will have to be filed with SISCO.

A secondary mitigation would be to utilize firewalls to perform IP-based filtering, ensuring that only specific trusted hosts are allowed to send traffic to the UCS ICCP server.

Zero Day Vulnerability: MMS Layer Invalid Pointer Dereference

There is a vulnerability in the *Icpe* process on the UCS host (*uc1inl*) that results in a invalid pointer dereference and subsequent crash of the ICCP communication stack. Sending a crafted Manufacturing Messaging Standard (MMS) Layer Data response to a read request, where the TASE2 version response field is set to zero, triggers the vulnerability. This particular vulnerability is likely not exploitable beyond allowing for a DoS; however, it may be possible with further investigation to identify a way of triggering the vulnerability in such a way as to allow for arbitrary code execution.

CVSS Baseline Metrics

Access Vector (AV)

The CVSS Access Vector rating is Network (N)—A vulnerability exploitable with network access means the vulnerable software is bound to the network stack, and the attacker does not require local network access or local access. Such a vulnerability is often termed “remotely exploitable.” CVSS Rating: AV:N

The vulnerability does not require local network access to attack. This vulnerability would be an example of the classically defined “remotely exploitable” vulnerability, accessible via routed (i.e., Layer 3 or the Network Layer in the OSI model) networks.

Access Complexity (AC)

The CVSS Access Complexity rating is Medium (M); access conditions are somewhat specialized. CVSS Rating: AC:M

The vulnerability requires an attacker to implement a non-trivial amount of the ICCP before being accessible. The attacker would also need to successfully identify the connection parameters needed to act as an ICCP peer to the target.

Authentication (Au)

The CVSS Authentication rating is None (N); authentication is not required to access and exploit the vulnerability. CVSS Rating: Au:N

Confidentiality Impact (C)

The CVSS Confidentiality Impact rating is None (N); there is no impact to the confidentiality of the system. CVSS Rating: C:N

Integrity Impact (I)

The CVSS Integrity Impact rating is None (N); there is no impact to the integrity of the system. CVSS Rating: I:N

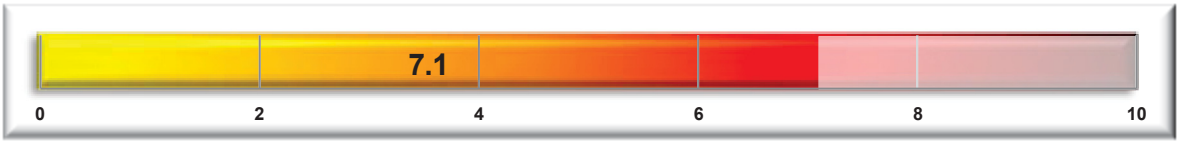
Availability Impact (A)

The CVSS Availability Impact rating is Complete (C); there is a total shutdown of the affected resource. CVSS Rating: A:C

The attacker can render the resource unavailable until a manual restart can be performed.

Vulnerability CVSS Score

Table 16. MMS layer invalid pointer dereference CVSS score.

Scoring Date:	**N/A**	 **CVSS Calculator**
Base Score	**7.1**	
Impact Subscore	6.9	
Exploitability Subscore	8.6	
Temporal Score	**Not Defined**	
Overall Score	**7.1**	
		
Vector	(AV:N/AC:M/Au:N/C:N/I:N/A:C)	

Mitigations

The primary mitigation method would be to perform bounds checking on all fields within the ICCP message, in accordance with best practice secure coding methods.

A workaround to limit exposure of this vulnerability would be to perform strict IP-based filtering, ensuring that only trusted hosts are allowed to send data to the UCS host. However, care should be taken with this approach as IP addresses can be spoofed, which limits the full effectiveness of IP (or other network token such as Domain Name Server [DNS]) based filtering.

Zero Day Vulnerability: MMS Layer Block 4 Message Heap Overflow

There is a vulnerability in the *Icpe* process on the UCS host (*uc1inl*) that results in a heap-based buffer overflow. The vulnerability occurs when processing a MMS layer Block 4 message that has an invalid, small size value combined with a long message string. A buffer is allocated based upon a size provided by the attacker, and then an attacker-controlled string is copied into that buffer. If the allocated buffer is smaller than the provided string, data next to the allocated buffer, which in this case contains heap structure control data, gets overwritten.

CVSS Baseline Metrics

Access Vector (AV)

The CVSS Access Vector rating is Network (N)—A vulnerability exploitable with network access means the vulnerable software is bound to the network stack, and the attacker does not require local network access or local access. Such a vulnerability is often termed "remotely exploitable." CVSS Rating: AV:N

The vulnerability does not require local network access to attack. This vulnerability would be an example of the classically defined "remotely exploitable" vulnerability, accessible via routed (i.e., Layer 3 or the Network Layer in the OSI model) networks.

Access Complexity (AC)

The CVSS Access Complexity rating is Medium (M); access conditions are somewhat specialized. CVSS Rating: AC:M

The vulnerability requires an attacker to implement a non-trivial amount of the ICCP before being accessible. The attacker would also need to successfully identify the connection parameters needed to act as an ICCP peer to the target.

Authentication (Au)

The CVSS Authentication rating is None (N); authentication is not required to access and exploit the vulnerability. CVSS Rating: Au:N

Confidentiality Impact (C)

The CVSS Confidentiality Impact rating is Complete (C); there is a total information disclosure, resulting in all system files being revealed. CVSS Rating: C:C

The attacker is able to read all of the system's data (memory, files, etc.).

Integrity Impact (I)

The CVSS Integrity Impact rating is Complete (C); there is a total compromise of system integrity. CVSS Rating: I:C

There is a complete loss of system protection, resulting in the entire system being compromised. The attacker is able to modify any files on the target system.

Availability Impact (A)

The CVSS Availability Impact rating is Complete (C); there is a total shutdown of the affected resource. CVSS Rating: A:C

The attacker can render the resource completely unavailable.

Vulnerability CVSS Score

Table 17. MMS layer Block 4 message heap overflow CVSS score.

Scoring Date:	**N/A**	 CVSS Calculator
Base Score	**9.3**	
Impact Subscore	10	
Exploitability Subscore	8.6	
Temporal Score	**Not Defined**	
Overall Score	**9.3**	
		
Vector	(AV:N/AC:M/Au:N/C:C/I:C/A:C)	

Mitigations

The primary mitigation method would be to perform bounds checking on all fields within the ICCP message, in accordance with best practice secure coding methods. More specifically, checks should be performed to ensure that the amount of data being copied into a dynamically allocated buffer to not exceed the bounds of that allocated buffer.

A workaround to limit exposure of this vulnerability would be to perform strict IP-based filtering, ensuring that only trusted hosts are allowed to send data to the UCS host. However, care should be taken with this approach as IP addresses can be spoofed, which limits the full effectiveness of IP (or other network token such as DNS) based filtering.

Zero Day Vulnerability: MMS Layer Block 4 Message Unhandled Memory Allocation DoS

There is a vulnerability in the *Icpe* process on the UCS host (*uc1inl*) that results in a DoS. Sending an invalid maximum size value for the Block 4 information object buffer can trigger the vulnerability. The crash results in an error message being printed to the system log describing a memory allocation error, and then termination of the ICCP stack and SISCO OSI Stack daemon.

CVSS Baseline Metrics

Access Vector (AV)

The CVSS Access Vector rating is Network (N)—A vulnerability exploitable with network access means the vulnerable software is bound to the network stack, and the attacker does not require local network access or local access. Such a vulnerability is often termed “remotely exploitable.” CVSS Rating: AV:N

The vulnerability does not require local network access to attack. This vulnerability would be an example of the classically defined “remotely exploitable” vulnerability, accessible via routed (i.e., Layer 3 or the Network Layer in the OSI model) networks.

Access Complexity (AC)

The CVSS Access Complexity rating is Medium (M); access conditions are somewhat specialized. CVSS Rating: AC:M

The vulnerability requires an attacker to implement a non-trivial amount of the ICCP before being accessible. The attacker would also need to successfully identify the connection parameters needed to act as an ICCP peer to the target.

Authentication (Au)

The CVSS Authentication rating is None (N); authentication is not required to access and exploit the vulnerability. CVSS Rating: Au:N

Confidentiality Impact (C)

The CVSS Confidentiality Impact rating is None (N); there is no impact to the confidentiality of the system. CVSS Rating: C:N

Integrity Impact (I)

The CVSS Integrity Impact rating is None (N); there is no impact to the integrity of the system. CVSS Rating: I:N

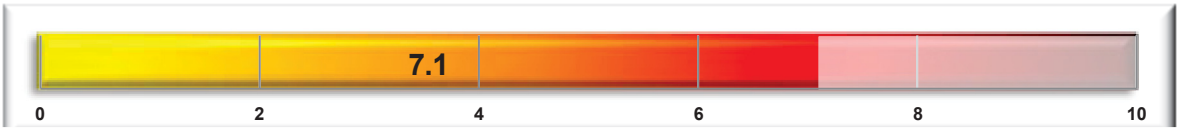
Availability Impact (A)

The CVSS Availability Impact rating is Complete (C); there is a total shutdown of the affected resource. CVSS Rating: A:C

The attacker can render the resource completely unavailable, until a manual restart of the service is performed.

Vulnerability CVSS Score

Table 18. MMS layer Block 4 message unhandled memory allocation DoS CVSS score

Scoring Date:	**N/A**	 **CVSS Calculator**
Base Score	**7.1**	
Impact Subscore	6.9	
Exploitability Subscore	8.6	
Temporal Score	**Not Defined**	
Overall Score	**7.1**	
		
Vector	(AV:N/AC:M/Au:N/C:N/I:N/A:C)	

Mitigations

The bug occurs when the *Icpe* application calls what appears to be an MMS-EASE method to allocate space for the Block 4 object buffer. The called method fails to allocate the overly large buffer, and returns an error, which is taken to mean that the application is out of memory, so the *Icpe* application quits.

The primary mitigation would be to follow secure coding practices, specifically detection of the invalid data before use. Doing so would prevent an invalid memory allocation error, which can be difficult to recover from gracefully, as it is frequently not clear as to why the allocation error occurred.

Zero Day Vulnerability: Large Outstanding Requests DoS

There is a vulnerability in the *Icpe* process on the UCS host (*uc1inl*) that results in a DoS. Sending an ICCP *init-request* message containing an overly large Number of Maximum Outstanding Requests triggers the DoS.

The invalid number of maximum outstanding requests is actually identified by one of the processes running on the UCS, but instead of handling the error gracefully, decides to terminate itself and subsequently the ICCP stack, causing the DoS.

CVSS Baseline Metrics

Access Vector (AV)

The CVSS Access Vector rating is Network (N)—A vulnerability exploitable with network access means the vulnerable software is bound to the network stack, and the attacker does not require local network access or local access. Such a vulnerability is often termed "remotely exploitable." CVSS Rating: AV:N

The vulnerability does not require local network access to attack. This vulnerability would be an example of the classically defined "remotely exploitable" vulnerability, accessible via routed (i.e., Layer 3 or the network layer in the OSI model) networks.

Access Complexity (AC)

The CVSS Access Complexity rating is Medium (M); access conditions are somewhat specialized. CVSS Rating: AC:M

The vulnerability requires an attacker to implement a non-trivial amount of the ICCP before being accessible. The attacker would also need to successfully identify the connection parameters needed to act as an ICCP peer to the target.

Authentication (Au)

The CVSS Authentication rating is None (N); authentication is not required to access and exploit the vulnerability. CVSS Rating: Au:N

Confidentiality Impact (C)

The CVSS Confidentiality Impact rating is None (N); there is no impact to the confidentiality of the system. CVSS Rating: C:N

Integrity Impact (I)

The CVSS Integrity Impact rating is None (N); there is no impact to the integrity of the system. CVSS Rating: I:N

Availability Impact (A)

The CVSS Availability Impact rating is Complete (C); there is a total shutdown of the affected resource. CVSS Rating: A:C

The attacker can render the resource completely unavailable, until a manual restart of the service is performed.

Vulnerability CVSS Score

Table 19. Large outstanding requests DoS CVSS score.

Scoring Date:	**N/A**	 **CVSS Calculator**
Base Score	**7.1**	
Impact Subscore	6.9	
Exploitability Subscore	8.6	
Temporal Score	**Not Defined**	
Overall Score	**7.1**	
		
Vector	(AV:N/AC:M/Au:N/C:N/I:N/A:C)	

Mitigations

As the invalid data within the init-request message is identified and even reported on, the primary suggested mitigation would be to send an appropriate error/terminate message to the peer that sent the invalid message.

A secondary mitigation would be to simply terminate the offending connection without messaging the peer.

Zero Day Vulnerability: MMS Layer Invalid Local Detail DoS

There is a vulnerability in the *Icpe* process on the UCS host (*uc1inl*) that results in a DoS. Sending an ICCP *init-request* message containing an overly large local detail field triggers the vulnerability.

CVSS Baseline Metrics

Access Vector (AV)

The CVSS Access Vector rating is Network (N)—A vulnerability exploitable with network access means the vulnerable software is bound to the network stack, and the attacker does not require local network access or local access. Such a vulnerability is often termed “remotely exploitable.” CVSS Rating: AV:N

The vulnerability does not require local network access to attack. This vulnerability would be an example of the classically defined “remotely exploitable” vulnerability, accessible via routed (i.e., Layer 3 or the network layer in the OSI model) networks.

Access Complexity (AC)

The CVSS Access Complexity rating is Medium (M); access conditions are somewhat specialized. CVSS Rating: AC:M

The vulnerability requires an attacker to implement a non-trivial amount of the ICCP before being accessible. The attacker would also need to successfully identify the connection parameters needed to act as an ICCP peer to the target.

Authentication (Au)

The CVSS Authentication rating is None (N); authentication is not required to access and exploit the vulnerability. CVSS Rating: Au:N

Confidentiality Impact (C)

The CVSS Confidentiality Impact rating is None (N); there is no impact to the confidentiality of the system. CVSS Rating: C:N

Integrity Impact (I)

The CVSS Integrity Impact rating is None (N); there is no impact to the integrity of the system. CVSS Rating: I:N

Availability Impact (A)

The CVSS Availability Impact rating is Complete (C); there is a total shutdown of the affected resource. CVSS Rating: A:C

The attacker can render the resource completely unavailable, until a manual restart of the service is performed.

Vulnerability CVSS Score

Table 20. MMS layer invalid local detail DoS CVSS score.

Scoring Date:	**N/A**	 **CVSS Calculator**
Base Score	**7.1**	
Impact Subscore	6.9	
Exploitability Subscore	8.6	
Temporal Score	**Not Defined**	
Overall Score	**7.1**	
		
Vector	(AV:N/AC:M/Au:N/C:N/I:N/A:C)	

Mitigations

As the invalid data within the init-request message is identified and even reported on, the primary suggested mitigation would be to send an appropriate error/terminate message to the peer that sent the invalid message.

A secondary mitigation would be to simply terminate the offending connection without messaging the peer.

5.6.6 Conclusions

One explicit heap-based buffer overflow was identified that could be exploited remotely to allow for remote arbitrary code execution. Five DoS vulnerabilities were identified, which could be exploited remotely to temporarily disable the ICCP service on the UCS host. It is possible that a couple of the DoS bugs can be converted into arbitrary code execution bugs, as the exploitability of each one was not fully evaluated.

One vulnerability was identified in the OSI stack that the UCS uses, developed by SISCO. The vulnerability is similar to an existing known vulnerability, which has been patched. If the issue is the same as the publicly known vulnerability, Siemens should contact SISCO for an updated version of the OSI stack software. If it is not the same, Siemens should work with INL in disclosing the information to SISCO such that a patch can be issued.

A couple of the DoS vulnerabilities were primarily the result of not checking values provided by the peer before their use, resulting in a handled error condition that ultimately caused the main ICCP process to terminate. If the data provided by the peer had been validated before use, the service would have been able to handle them appropriately as opposed to dealing with an ambiguous error condition.

In all cases, secure coding practices regarding validating external data before use would mitigate each of the vulnerabilities identified. There are likely a number of other vulnerabilities that were not uncovered in testing. A code audit and further testing is recommended to help minimize security issues.

5.7 Target 7 – Phase 1 Patch Verification

5.7.1 Introduction

The objective of this assessment target was to evaluate vulnerabilities identified in the Phase 1 Power 3 assessment performed at INL to verify that they had been patched, and if so, evaluate the efficacy of the patch. In 2007, INL performed an assessment of the Siemens Spectrum Power 3.9 system. The results of this testing were reported to Siemens for evaluation and resolution of potential risks. Four years later, Siemens sent their latest Spectrum Power system, Version 3.10, to INL for another round of security testing.

This section attempts to extract the pertinent information from the Cyber Researcher's report on AT7. The Cyber Researcher's report documents to a level where "someone similarly skilled in the art" can reproduce the results. This level is not required for the general report. For the reader that needs this level of detail, read the attached Cyber Researcher's report: AT7 – Phase 1 Patch Verification.

AT7 - Validation of Phase 1.pdf

5.7.2 Objective

This assessment target's objective is to assess whether the vulnerabilities identified in Phase 1 testing have been mitigated in the subsequent Power 3.10 system.

5.7.3 Significance

Validation of Siemens' mitigations to security issues found in the previous assessment gives Siemens assurance that their solutions are effective and gives the DOE assurance that their processes are increasing the security of SCADA systems used in the nation's critical energy infrastructure. In the case that a security risk was not adequately reduced, INL can provide additional recommendations.

5.7.4 Rules of Engagement

There were no rules of engagement that impacted this portion of the assessment.

The system under test did not include typical perimeter connections to attack from (i.e., a corporate network and firewall, DMZ, vendor connection, modem pool, or ICCP connection) since the focus of the assessment project was to determine the cyber security posture of the core system hardware and software

configuration. Therefore, the assessment was conducted from INL computers connected directly to the Power 3 EMS/SCADA and RTU communications network.

5.7.5 Assessment

The previous assessment assessed the security of each of the following Spectrum Power 3.9 system hosts:

- The Administrator Data Management (ADM)/Oracle server
- The Communications server (COM)
- The User Interface/ Man-Machine Interface (UI/MMI) server
- Transmission Operator Workstation (Windows UI)
- The Communications Front-End (CFE) server
- The Historical Server (HIS)
- The Communications Application (CA)/ICCP server
- The Real-Time Data Server (RTDS).

The Power 3 software was also evaluated for vulnerabilities that would allow access to the SCADA system.

The Spectrum Power 3.10 system under test is comprised of a Windows PC for UI access and the following AIX virtual hosts:

- ADM server
- COM server
- Transmission Network Applications (TNA) server
- Utility Communications Server (UCS)
- CFE
- Remote Front End (RFE) server
- UI server.

The Spectrum Power 3.9 and 3.10 host configurations were compared to the recommended host configurations in the Siemens *Power 3 Security Administration and Maintenance, User Guide*.

5.7.5.1 Method 1: Host Evaluation

Spectrum Power 3.9 Finding: Unused Services

The host operating systems were configured by Siemens for the Spectrum Power 3.9 and Power 3.10 systems using their standard configuration practices. The system computers were scanned for vulnerabilities and open ports using freely available security tools, nmap, and Nessus.

Open ports are services available for use on the network. “An application is actively accepting TCP connections, User Datagram Protocol (UDP) datagrams or SCTP associations on this port. Finding these is often the primary goal of port scanning. Security-minded people know that each open port is an avenue for attack. Attackers and pen-testers want to exploit the open ports, while administrators try to close or protect them with firewalls without thwarting legitimate users.” (Lyon, Gordon “Fyodor,” Port Scanning Basics, http://nmap.org/book/man-port-scanning-basics.html)

Spectrum Power 3.10 Solution to Unused Services Finding

The Spectrum Power 3.10 hosts have fewer services listening on the network than the Spectrum Power 3.9 assessment system hosts and are therefore less exposed to attack. All available services were listed as required in the *Power 3 Security Administration and Maintenance, User Guide*.

Siemens produced the following security configuration guides that list required services:

- Power 3 Installation Guide, Core System: AIX 5.3 installation for Power 3
- Power 3 Security Administration and Maintenance, User Guide.

The Power 3 Security Administration Toolkit configuration script can be used to secure the AIX operating system. "Services and daemons to be turned off or on by the security toolkit are specified in the services_conf configuration file, which can be edited by the Power 3 customer."

Recommendations

Siemens should validate that all services, applications, and libraries are patched and up to date when delivering a new system. Siemens should also encourage and support customers in monitoring for and applying security updates and patches for the services, applications, and libraries used by the Power 3 system.

Spectrum Power 3.9 Finding: Clear-Text Authentication Protocols

One of the most significant and widespread issues the assessment team identified on the Spectrum Power 3.9 test system was the use of plain-text network protocols, along with misconfigured services. As such, the content of the system's communication packets can be intercepted, read, and manipulated. This includes usernames, passwords, and SCADA commands. The Spectrum Power 3.9 test system was running the following plain text authentication protocols: rsh, rexec, rlogin, telnet, File Transfer Protocol (FTP), Softbus, and Distributed Network Protocol Version 3 (DNP3).

Spectrum Power 3.10 Solution to Clear-Text Authentication Protocols Finding

The Spectrum Power 3.10 assessment system hosts are not running the clear-text authentication protocols rsh, rexec, rlogin, telnet, and FTP.

Softbus traffic is encrypted using Transport Layer Security (TLS).

Distributed Network Protocol Version 3 (DNP3) traffic is in clear text.

Spectrum Power 3.9 Finding: NFS

Most of the AIX machines on the Spectrum Power 3.9 assessment system used NFS servers with only IP-based authentication. An attacker could gain access to the shared drives by spoofing an authorized IP address.

NFS access control is performed by specifying the names or IP addresses of machines that are allowed to access a share point. If someone is capable of spoofing or taking over a trusted address then they can access the mount points.

File system access controls for files on an NFS shared drive can be circumvented by the NFS client. Once a drive is mounted, the user and group permissions on the files determine access control based on the user ID specified by the client.

Spectrum Power 3.10 NFS Implementation

An attacker is still able to spoof a trusted IP address and mount the Spectrum Power 3.10 /home directory.

Configuration-Induced Vulnerability: Power 3 files accessible via NFS

The Spectrum Power 3.10 system ADM, COM, TNA, UCS, and CFE NFS servers export the following shares:

- /home main-net
- /home/cores main-net.

The assessment team was able to mount /home on each of these servers by spoofing the IP of one of the hosts in the main-net group.

CVSS Baseline Metrics

Access Vector (AV)

The CVSS Access Vector rating is Adjacent Network (A)—A vulnerability exploitable with *adjacent network access* requires the attacker to have access to either the broadcast or collision domain of the vulnerable software. CVSS Rating: AV:A

Access Complexity (AC)

The CVSS Access Complexity rating is Low (L); specialized access conditions or extenuating circumstances do not exist. CVSS Rating: AC:L

Authentication (Au)

The CVSS Authentication rating is None (N); authentication is not required to access and exploit the vulnerability. CVSS Rating: Au:N

Confidentiality Impact (C)

The CVSS Confidentiality Impact rating is Partial (P); there is considerable informational disclosure. CVSS Rating: C:P

Integrity Impact (I)

The CVSS Integrity Impact rating is Partial (P); modification of some system files or information is possible. CVSS Rating: I:P

Availability Impact (A)

The CVSS Availability Impact rating is Complete (C); there is a total shutdown of the affected resource. CVSS Rating: A:C

An attacker an overwrite files that are necessary for system operation.

Vulnerability CVSS Score

Table 21. Power 3 files accessible via NFS CVSS score.

Scoring Date:	**N/A**	 **CVSS Calculator**
Base Score	**7.3**	
Impact Subscore	8.5	
Exploitability Subscore	6.5	
Temporal Score	**Not Defined**	
Overall Score	**7.3**	
		
Vector	(AV:A/AC:L/Au:N/C:P/I:P/A:C)	

Mitigations

The recommended mitigations for this vulnerability are as follows: do not export directories that do not need to be exported; prevent access to NFS server ports on all hosts that do not need to export directories; and tunnel NFS over SSH or upgrade to NFS Version 4 and configure the system to use its authentication and encryption security options.

Spectrum Power 3.9 Finding: Vulnerable SSH Implementation

The Spectrum Power 3.9 system SSH implementation had three problems:

4. The authorized_keys file allows any computer with a known public key to log in without a password.
5. The private keys are left unencrypted.
6. The private keys for PC01 and PC02 are stored on computers other than PC01 and PC02, respectively.

The authorized_keys file lists the public keys that can be used without additional authentication. The idea behind this is that the corresponding private key is well-protected, and the public key is only usable if the private key is also known. If the private key is compromised, any computer with the corresponding public key as an authorized_key is also compromised.

The private keys for SSH should be kept encrypted to help prevent compromise. To get a machine's private key, the system must first be compromised; however, once one machine is compromised, all of the machines running an SSH daemon within established trust relationships are compromised because the first machine left its private key unencrypted.

Storing other systems' private keys creates a single point of failure. Private keys are named private because no other point needs to know them; therefore, there is no reason to have other machine's private keys.

Spectrum Power 3.10 SSH Implementation

The Spectrum Power 3.10 system still uses the authorized keys file and private keys are left unencrypted. This configuration is needed for Power 3 scripts to be able to use SSH instead of Remote Shell (RSH) (or any other plain-text authentication protocol) without user interaction.

The permissions of the private keys on the AIX hosts make them only accessible by the account owner. NFS uses the user ID and group ID of the client to control access to the exported file system. This means that an attacker with the same user ID as spsy can read the spsy and pc01inl SSH private keys.

Configuration-Induced Vulnerability: SSH private keys shared via NFS

The spsy account and pc01inl private keys are stored under the /home directory on the AIX hosts. These private keys can be copied by anyone able to NFS mount the /home directory. Possession of the spsy private keys allows the holder to SSH to any of the Power 3 AIX hosts as the spsy user without providing a password. The pc01inl private key can be used to access the Windows host, pc01inl.

Recommendations

Do not store private keys on an NFS export. Make sure that all private keys are well protected.

Concern: SSH restrictions can be circumvented

SSH access is restricted by the `sshcheck_deny` file. This file attempts to deny remote shell access to the root, spsy, and imdba users via SSH by preventing them from running `ksh` with no arguments.

Recommendations

The assessment team recommends creating a complete white list of the full commands that are required by the Power 3 scripts, enumerating these required commands into the sshcheck_allow file, and restricting everything in the sshcheck_deny file (because allow takes precedence over deny.)

It is also important to note that script used to enforce these restrictions, sshcheck.pl, is located under the NFS shared directory and can be edited by an unauthorized remote attacker. Potential mitigations include the following:

- Move the sshcheck.pl script to a secure location
- Do not export the /home directory
- Securely implement NFS Version 4
- Tunnel NFS over SSH.

Spectrum Power 3.9 Finding: Vulnerable X11 Implementation

On the Spectrum Power 3.9 assessment system, the initial configurations of the ADM and MMI servers had X server implementations that accepted clients from anywhere. This allows anyone to connect to the X session and record keystrokes and screenshots. After the system was rebuilt, the X server did not allow the test client to connect to it, raising the issue of whether the system was properly configured to start with.

Even when the X11 authentication was restricted to IP addresses listed in the /etc/hosts file, the assessment team was able to connect to any of the AIX host's X-servers and record keystrokes and screenshots by configuring their address as one listed in the /etc/hosts file.

Spectrum Power 3.10 Solution to X11 vulnerabilities

The Spectrum Power 3.10 system is configured to forward all X11 traffic through SSH. Siemens provides documentation and tools to aid in configuring the X server and firewalls to prevent remote access to X11 Transmission Control Protocol (TCP) Port 6000.

It was not possible to directly connect to the X servers as was done on the previous assessment.

Concern: X11 port forwarding through SSH implementation

Spectrum Power 3 Security Administration and Maintenance, User Guide, Appendix F, Required Ports, lists TCP Port 6000 as only being required on the MMI, and that it should only be listening to localhost. "All X traffic is tunneled through ssh, this should only be listening to the localhost." The UI and ADM should be running an Xserver on TCP Port 6009, listening only to localhost.

Spectrum Power 3 Security Administration and Maintenance, User Guide, Appendix G, lists daemons on Power 3 hosts. X is only listed under the MMI.

Nmap scans do not show TCP Port 6000 listening on any of the hosts, but the netstat command shows all hosts listening on all interfaces (*.6000), accepting connections from any address (*.*).

Recommendations

The assessment team recommends disabling the X server on the hosts that do not require it and configuring the X server to only listen on localhost.

Method Conclusions

For the previous assessment, Siemens did not provide a listing of ports and services required for system operation to the INL team. They were in the process of developing a methodology for providing this information to customers. A security administration and maintenance guide was included with the Spectrum Power 3.10 system. Although a security toolkit is included with the Power 3 system, it was not used to configure either of the assessment systems.

In general, the configuration of AIX on the servers in the previous system configuration allowed easy access once on the SCADA system network. Specifically, the assessment team identified vulnerabilities with clear-text protocols, NFS, X11, and SSH that would assist an attacker in gaining access to the SCADA system.

The number of open ports on the Spectrum Power 3.10 assessment system is greatly reduced. The only open ports that were not listed as required were the NFS TCP and UDP ports.

The NFS implementation on the Spectrum Power 3.10 system still only utilizes IP and user ID-based authentication, which can be circumvented. The directories exported via NFS should be limited to those necessary for system operation. NFS should be either tunneled over SSH or configured to use NFS Version 4 and its authentication and encryption security options.

SSH private keys and the certificates used for SSL authentication are located on NFS exports. Private keys and certificates should be well protected. In the current configuration, they can be copied by anyone able to NFS mount the /home directory. The private keys are not encrypted and can be used to authenticate to the Power 3 hosts without a password. The SSL certificates are encrypted with a password, which was cracked by the assessment team.

SSH private keys are used by Power 3 scripts to SSH without supplying a hard-coded, plaintext password. Restrictions are placed on the root, spsy, and imdba users to only allow the functionality needed by these scripts. SSH restrictions meant to prevent root, spsy, or imdba RSH access can be circumvented.

On the Spectrum Power 3.9 assessment system, the initial configurations of the ADM and MMI servers had X server implementations that accepted clients from anywhere. The Spectrum Power 3.10 system is configured to forward all X11 traffic through SSH. Access to Port 6000 is filtered, but Power 3 hosts should be configured to only accept Port 6000 connections from localhost as a layer of defense.

5.7.5.2 Method 2: Evaluate Mitigations for Softbus Vulnerabilities

Most Power 3 programs communicate with one another by using the Softbus protocol. Softbus allows a program to send messages to programs on other servers.

Spectrum Power 3.9 Finding: Weak Softbus Authentication

The Spectrum Power 3.9 assessment team found that Softbus uses the hard-coded entries in the /etc/hosts file to authenticate network hosts. Attributes, in addition to address/name tuples, are contained therein. For example:

```
192.168.0.1 hostname ea1=8:0:2:1:2:3 lic=123456 …
```

The license key for that host was in the /etc/hosts file. In the Spectrum Power 3.9 system installation, the entries were added to one of the Power 3 system's /etc/hosts file, then that file was propagated to all the machines in the system.

To decide whether a host can connect to another, the IP addresses are compared numerically (i.e., 10.2.3.4 can connect to 10.2.3.5 via Softbus, but not the other way around). Connections initiated from the lower IP address are accepted then promptly closed. Therefore, a good place to be is on the highest "blessed" IP address available (by being in the /etc/hosts files). This is the only form of authentication required to join the Softbus network and it is easily defeated.

During testing, an assessment team laptop was connected to the primary control system Local Area Network (LAN). Simple Address Resolution Protocol (ARP) poisoning was used to "steal" the address of the CA machine. Attacks were then mounted against the ADM and RTDS servers. The CA machine was an ideal machine to attack because its address is numerically larger than that of the other machines, allowing the team to bypass the only form of authentication in use.

A Softbus decoder was written that could take intercepted Softbus traffic and provide the details of all passed messages. This data could then be stored for later use or manipulated and passed along to the correct endpoint.

Spectrum Power 3.10 Softbus Authentication Solution

The approach taken by Power 3 is to use the TLS protocol to transmit the data. The data may be encrypted or TLS may be used to authenticate the message.

Softbus can now run in three different modes:

- Plain TCP sends everything unauthenticated and not encrypted. It is not secure because it can be tampered with.
- TLS with authentication authenticates the message only. TLS uses certificates to authenticate Softbus messages.
- TLS with encryption encrypts the message.

Concern: Softbus security downgrade via NFS export

The buls.conf file, used to set the Softbus security preferences, is located on the NFS exported directory. It is possible to change the Softbus security options, which set the security modes that the Power 3 server will support in the buls.conf file via NFS. The new settings will take effect when BULS is restarted. This method was used by the assessment team to downgrade Softbus communications from encrypted to plaintext.

Spectrum Power 3.9 Finding: Softbus Shared Memory Transfer (SBXFER)

The second layer of Softbus allows for the transfer of shared memory segments between Softbus peers. This functionality is the primary mechanism by which Softbus peers exchange data and is a critical aspect of the Power 3 system's functionality. No authentication is required other than that of having a blessed IP address.

By carefully crafting packets, any writable part of memory in the BULS process can be overwritten. An attack was written that installed itself and overwrote part of the environment pointer array (located near the top of the stack at a largely fixed offset). To get the code to execute, a function pointer was set to point to the code. The attack bound to a socket, and started a shell with the privileges of the BULS server: root. This attack leaves the BULS process running normally and gives full system privileges to the attacker. Any system running the BULS server, which would be any Softbus peer in the system, is a potential target of this attack.

Another aspect of this attack vector is that any portion of the shared memory could be altered. This would enable an attacker to alter data or messages between Softbus peers. Some reasons for doing this would include:

- Feeding normal looking data to an operator's console when in reality something bad is happening
- Altering operator commands
- Manipulating an application that peers through Softbus.

The only obstacle to performing any of these attacks lies in understanding the messaging format for the targeted functionality.

Spectrum Power 3.10 SBXFER status

The BULS program now runs as the spsy user in the Version 3.10. This means that an attacker could only gain spsy privileges instead of root.

TLS greatly increases the difficulty of this attack, but the Softbus Shared Memory Transfer (SBXFER) vulnerability may still exist.

The NFS shares provide at least two ways to circumvent the TLS authentication/encryption added to Softbus. The NFS shares allow access to the SSL certificates needed to authenticate via TLS. The buls.conf security configuration file is also available on the NFS share.

The assessment team used the NFS share to edit the buls.conf file on the COM to change the security options from preferring to use encryption to only accepting plain TCP connections. The exploits used on the previous assessment were not successfully launched against the Spectrum Power 3.10 system, but the assessment team is not convinced that the vulnerability does not still exist. Additional time is required to edit the exploit used against the Spectrum Power 3.9 system.

Spectrum Power 3.9 Finding: BULS DoS Vulnerability

BULS is the Softbus communication management process.

The code in the file tiso.c implements the first layer of the Softbus protocol. It handles four message types that are designed to make TCP look like an Open Systems Interconnection (ISO) stack. Messages with a type of cTCPconf (type 0xff98) are vulnerable to a crash. It appears that the data portion of the message is used, without verification, as an index into an array. Setting the index to a negative value will crash BULS.

Spectrum Power 3.10 BULS DoS status

BULS is still vulnerable to DoS via cTCPconf messages.

TLS authentication decreases the exploitability of this vulnerability. An attack must come from an authorized Power 3 host.

CVSS Baseline Metrics

Access Vector (AV)

The CVSS Access Vector rating is Network (N); a vulnerability exploitable with network access means the vulnerable software is bound to the network stack, and the attacker does not require local network access or local access. Such a vulnerability is often termed "remotely exploitable." CVSS Rating: AV:N

Access Complexity (AC)

The attacking party is limited to a group of systems or users at some level of authorization.

The CVSS Access Complexity rating is Medium (M); access conditions are somewhat specialized. CVSS Rating: AC:M

Authentication (Au)

The CVSS Authentication rating is None (N); authentication is not required to access and exploit the vulnerability. CVSS Rating: Au:N

Confidentiality Impact (C)

The CVSS Confidentiality Impact rating is None (N); there is no impact to the confidentiality of the system. CVSS Rating: C:N

Integrity Impact (I)

The CVSS Integrity Impact rating is None (N); there is no impact to the integrity of the system. CVSS Rating: I:N

Availability Impact (A)

The CVSS Availability Impact rating is Complete (C); there is a total shutdown of the affected resource. CVSS Rating: A:C

Vulnerability CVSS Score

Table 22. BULS DoS vulnerability CVSS score.

Scoring Date:	**N/A**	 **CVSS Calculator**
Base Score	**7.1**	
Impact Subscore	6.9	
Exploitability Subscore	8.6	
Temporal Score	**Not Defined**	
Overall Score	**7.1**	
		
Vector	(AV:N/AC:M/AU:N/C:N/I:N/A:C)	

Mitigation

The vulnerability still exists and can be exploited through an authorized host or by spoofing an authorized IP address if TLS is not used. Input validation should be added to the code to test that the provided value is within bounds.

Method Conclusions

The Spectrum Power 3.9 assessment team found that Softbus protocol relied on IP-based authentication, which is easily defeated. A Softbus decoder was written that could take intercepted Softbus traffic and provide the details of all passed messages. This data could then be stored for later use or manipulated and passed along to the correct endpoint.

The Spectrum Power 3.10 system provides three Softbus security options:

- Plain TCP (unauthenticated and not encrypted)
- TLS with authentication
- TLS with encryption.

The Softbus security preferences configuration file is available for editing via NFS. It is possible to change the Softbus security options that set the security modes the server will support in the buls.conf file via NFS. This method was used by the assessment team to downgrade Softbus communications from encrypted to plaintext.

Once the Softbus messages were not wrapped with TLS, the assessment team tested for the BULS TISO cTCPconf DoS vulnerability. The same exploit code used in the previous assessment was used to crash the BULS server.

TLS authentication and encryption make it harder to exploit the Spectrum Power 3.10 system. However, the primary mitigation for input validation vulnerabilities is to fix the source code. TLS is a secondary mitigation (part of the defense in depth).

5.7.5.3 Method 3: Evaluate DNP 3 Network Traffic

The Phase 1 assessment monitored the DNP3 protocol communications to assess the vulnerability to a direct network attack.

The technique chosen to attempt data subversion is known as an ARP Man-in-the-Middle (MitM) attack. This technique uses the ARP to trick the endpoints in a given network conversation to send their output to the attacker instead of each other. In this case, DNP3 between the CFE and the RTU was intercepted and analyzed.

DNP3 is a common SCADA protocol, supported by the Power 3 system. The protocol itself does not support authentication or access control. Siemens provides network applications on the CFE and Station Manager RTU, which allow them to communicate via DNP3.

Spectrum Power 3.9 Finding: DNP 3 MIM

A DNP3 decoder module was written to extract data values associated with point numbers/types for all DNP3 traffic that INL has analyzed. These values were kept in a local data store, available for future use as a replayable source of historically correct data or altered and reused as an attacker might require. The availability of accurate historical data can make it possible for an attacker to provide misleading data while an attack is conducted, keeping system operators from knowing the true state of the process.

Using the DNP3 decoder developed in the protocol discovery phase of testing, traffic between the CFE and RTU was intercepted and manipulated to cause the values displayed on the operator's screen to be whatever the attacker wants them to be. The decoder also accepted command-line input to force a point's value in the RTU.

Spectrum Power 3.10 DNP 3 Implementation

The Spectrum Power 3.10 assessment system communicates with a Siemens Station Manager RTU via plain-text DNP3. No message confirmation or access controls are in place to restrict access to the RTU.

Recommendations

System designers can make it more difficult to attack a system employing DNP3 by requiring implementation of message confirmation. Another method that can help is to configure the field equipment to only allow connections from the IP addresses of the systems that are expected to connect to those devices, if the equipment supports this.

Method Conclusions

DNP3 is a common SCADA protocol, supported by the Power 3 system. Siemens provides network applications on the CFE and Station Manager RTU, which allow them to communicate via DNP3. The protocol itself does not support authentication or access control. Traffic between the CFE and RTU can be intercepted and manipulated to cause the values displayed on the operator's screen to be whatever the attacker wants them to be. DNP3 messages to the RTU can be altered to force a point's value in the RTU.

5.7.6 Conclusions

In 2007, INL performed an assessment of the Siemens Spectrum Power 3.9 system. The results of this testing were reported to Siemens for evaluation and resolution of potential risks. Two years later, Siemens sent their latest Spectrum Power system, Version 3.10, to INL for another round of security testing. This assessment target's objective was to assess whether the vulnerabilities identified in Phase 1 testing have been mitigated in the subsequent Spectrum Power 3.10 system.

Siemens did not provide the INL team with a listing of ports and services required for Spectrum Power 3.9 system operation. They were in the process of developing a methodology for providing this information to customers. A security administration and maintenance guide was included with the Spectrum Power 3.10 system. Although a security toolkit is included with the Power 3 system, it was not used to configure either of the assessment systems.

In general, the configuration of AIX on the servers in the previous system configuration allowed easy access once on the SCADA system network. Specifically, the assessment team identified vulnerabilities with clear-text protocols, NFS, X11, and SSH, that would assist an attacker in gaining access to the SCADA system.

The number of open ports on the Spectrum Power 3.10 assessment system is greatly reduced. The only open ports that were not listed as required were the NFS TCP and UDP ports.

The integrity, availability, and confidentiality of all Power 3 files exported via NFS are at risk. The NFS implementation on the 3.10 system still only utilizes IP and user ID-based authentication, which can be circumvented. The directories exported via NFS should be limited to those necessary for system operation. NFS should be either tunneled over SSH or configured to use NFS Version 4 and its authentication and encryption security options.

SSH private keys and the certificates used for SSL authentication are located on NFS exports. Private keys and certificates should be well protected. In the current configuration, they can be copied by anyone able to NFS mount the /home directory. The private keys are not encrypted and can be used to authenticate to the Power 3 hosts without a password. The SSL certificates are encrypted with a password that was cracked by the assessment team.

SSH private keys are used by Power 3 scripts to SSH without supplying a hard-coded, plaintext password. Restrictions are placed on the root, spsy, and imdba users to only allow the functionality needed by these scripts. SSH restrictions meant to prevent root, spsy, or imdba remote shell access can be circumvented.

On the Spectrum Power 3.9 assessment system, the initial configurations of the ADM and MMI servers had X server implementations that accepted clients from anywhere. The Spectrum Power 3.10 system is configured to forward all X11 traffic through SSH. Access to Port 6000 is filtered, but Power 3 hosts should be configured to only accept Port 6000 connections from localhost as a layer of defense.

Most Power programs communicate with one another by using the Softbus protocol. Softbus allows a program to send messages to programs on other servers. BULS is the Softbus communication management process.

The Spectrum Power 3.9 assessment team found that Softbus protocol relied on IP-based authentication, which is easily defeated. A Softbus decoder was written that could take intercepted Softbus traffic and provide the details of all passed messages. This data could then be stored for later use or manipulated and passed along to the correct endpoint.

The Spectrum Power 3.10 system provides three Softbus security options:

- Plain TCP (unauthenticated and not encrypted)
- TLS with authentication
- TLS with encryption.

The Softbus security preferences configuration file is available for editing via NFS on the ADM, COM, TNA, UCS, and CFE. It is possible to change the Softbus security options, which set the security modes these servers will support in the buls.conf file via NFS. This method was used by the assessment team to downgrade Softbus communications from encrypted to plaintext.

Once the Softbus messages were not wrapped with TLS, the assessment team tested for the BULS cTCPconf DoS vulnerability. The same exploit code used in the previous assessment was used to crash the BULS server.

The assessment team was not able to adequately test whether the SBXFER vulnerability had been remediated in the time allocated. Additional time is required to edit the exploit used against the Spectrum Power 3.9 system.

TLS authentication and encryption make it harder to exploit the Spectrum Power 3.10 system. However, the primary mitigation for the BULS input validation vulnerabilities is to fix the BULS code. TLS is a secondary mitigation (part of the defense in depth).

DNP3 is a common SCADA protocol, supported by the Power 3 system. Siemens provides network applications on the CFE and Station Manager RTU, which allow them to communicate via DNP3. The protocol itself does not support authentication or access control. Traffic between the CFE and RTU can be intercepted and manipulated to cause the values displayed on the operator's screen to be whatever the attacker wants them to be. DNP3 messages to the RTU can be altered to force a point's value in the RTU.

Table 23 summarizes the status of the findings reported on the Spectrum Power 3.9 system. Green indicates Phase 1 vulnerabilities that have been tested and found to be patched. Red indicates Phase 1vulnerabilities that have not been patched.

Table 23. Summary of Spectrum Power 3.9.3 reported vulnerabilities.

3.9.3 Assessment Findings	3.10 Status
Unused services	Security guide lists necessary services
Power 3 directory available via NFS	NFS still available on ad1inl, cm1inl, na1inl, uc1inl, and cf1inl
Clear-text protocols	Clear-text authentication protocols not installed
The hosts.equiv configuration file allows rsh, rlogin, and rcp access without a password	rsh, rlogin, and rcp replaced with SSH
SSH configuration: 1. Authorized_keys file allows any computer with a known public key to log in without a password. 2. Private keys are left unencrypted. 3. Private keys for MMI computer PC01 are defined, but non-existent, PC02 private keys are stored on computers other than PC01 and the non-existent PC02, respectively.	1. Authorized_keys file allows any computer with a known public key to log in without a password. 2. Private keys are left unencrypted. 3. Private keys are available via NFS
Open X server	X11 traffic is tunneled over SSH X11 Port 6000 is still listening on the network
Ability to spoof or alter data in the Softbus messages	TLS authentication and encryption are available for Softbus Softbus security options can be set via NFS
Softbus Shared Memory Transfer	Not validated
BULS DoS vulnerability	Still vulnerable
Ability to alter values between CFE and RTU	MitM of DNP3.0 traffic is still possible

6 ASSESSMENT SUMMARY

The purpose of this assessment was to identify vulnerabilities that exist in the Phase 2 configuration of the Siemens Spectrum Power 3 system and make recommendations to mitigate those vulnerabilities in the interest of protecting the critical infrastructure controlled by Power 3 systems from cyber attack.

As listed in Section 4.3, and detailed in Section 5, this assessment found vulnerabilities in multiple categories, as shown in Figure 4.

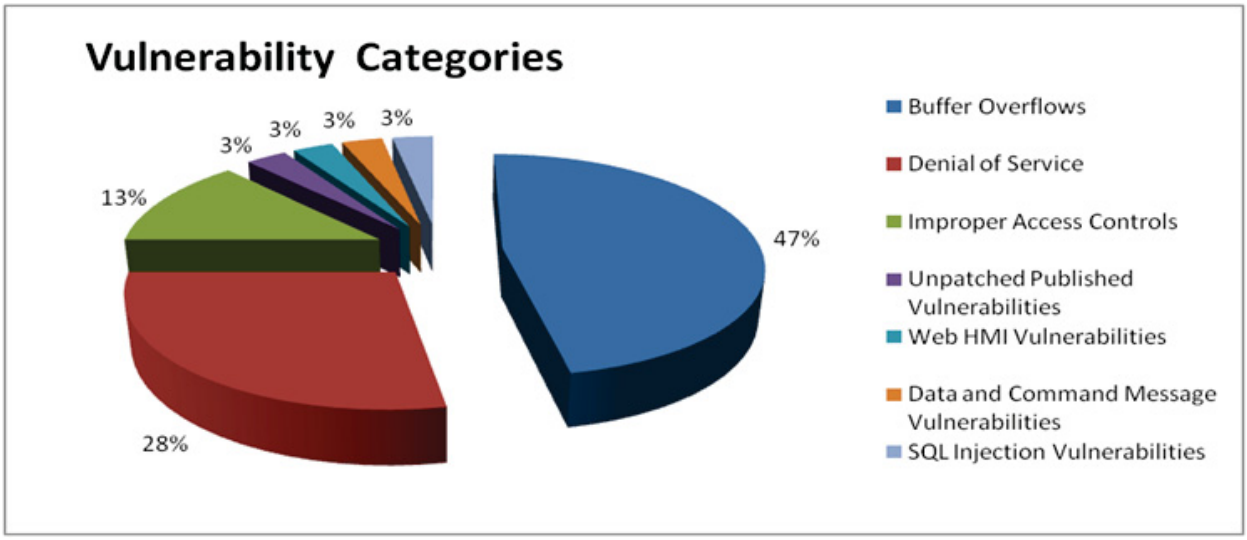


Figure 4. Assessment vulnerability category breakdown.

The vulnerability categories and associated mitigations that may be implemented to minimize their risk to this control system vulnerability are listed below:

- 47% of the vulnerabilities found in this assessment are buffer overflows, which can be mitigated by input validation
- 28% of the vulnerabilities found in this assessment are Denial of Service (DoS) vulnerabilities, which can be mitigate d by input validation
- 13% of the vulnerabilities are improper access control vulnerabilities (authorization), which can be mitigated by locking down all applications, hosts, and networks to limit the consequences of compromise as much as possible
- 3% of the vulnerabilities are unpatched published vulnerabilities, which can be mitigated by routinely assessing all SCADA components, including operating systems, applications, services, network devices, etc., for published vulnerabilities
- 3% of the vulnerabilities are Web HMI vulnerabilities, which can be mitigated by assessing how Web servers handle information provided by clients
- 3% of the vulnerabilities are SCADA data and command message manipulation and injection vulnerabilities, which can be mitigated by redesigning SCADA network protocols and the service applications that implement them for security
- 3% of the vulnerabilities are SQL injection vulnerabilities, which can be mitigated by protecting SCADA databases through input validation and filtering.

Overall, the assessment team found that most vulnerabilities from Phase 1 testing have been mitigated, but new vulnerabilities requiring further mitigation were found in Phase 2. In addition to these

vulnerabilities, the team also found noteworthy security practices and improvements in the Power 3 system since the conclusion of Phase 1 testing. The Power 3 System has shown a positive progression toward secure systems; however, as mentioned in the Executive Summary, it is strongly encouraged that Siemens continue the process of security assessments and testing.

7 AFTER ACTION REPORT

An After Action Report (AAR) is required from Siemens to document the mitigations and improvements made to the Siemens Basic System Platform based on the cyber security assessment in regard to control system security. This information provides a valuable metric on the relative progress that DOE-OE's Cyber Security for Energy Delivery Systems research and development program is making in respect to securing the control systems deployed in the Energy sector. The AAR will include the identified vulnerabilities, actions taken for mitigation, patches developed and deployed, full system deployments with updated security measures based off the findings, and any alerts or bulletins that were delivered to the vendors' user communities for awareness. If an identified vulnerability was not addressed, DOE-OE would like to know what your path forward is to address it.

7.1 Products

A final AAR will be provided to DOE-OE through the Assessment Lead, on mitigation and security practices implemented to address the vulnerabilities that were identified in this assessment report. Content of the AAR will include:

- Identified vulnerability
- Vulnerability ranking
- Action taken for each vulnerability
- Patches developed and deployed for vulnerabilities
- Increased security practices/technologies within the product line
- Alerts and bulletins
- Vulnerabilities not addressed and path forward to mitigate.

7.2 Deliverable Schedule/Process

The delivery schedule and process must be followed to secure the information and provide a status update on actions taken to reduce the risk to critical infrastructure and provide more secured systems to industry.

The AAR is due 6 months after the original delivery date of the assessment report. A secured delivery of the AAR will be required to protect the data; Pretty Good Privacy is a preferred method with key exchange to provide for encryption capabilities.