National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

Siemens Canada Ltd.

RUGGEDCOM Rugged Operating System (ROS)

V4.2.2.F

Running on the M2100F, M2200F, M969F, RSG2100F, RSG2100PF, RSG2200F, RSG2300F, RSG2300PF, RSG2488F, RS400F, RS416F, RS416PF, RS900F, RS900GF, RS900GPF, and RS940GF RUGGEDCOM switches

Report Number: CCEVS-VR-VID10877-2018

Dated: August 21, 2018

Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Jerome F. Myers, Ph.D.
James Donndelinger
The Aerospace Corporation

Common Criteria Testing Laboratory

Dragua Zenelaj
Rory Saunders
Curtis Cobb
Aditya Patil
COACT, Inc.

Table of Contents

List Of Tables

1. Executive Summary

This Validation Report (VR) documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the RUGGEDCOM Rugged Operating System (ROS) v4.2.2.F running on the M2100F, M2200F, M969F, RSG2100F, RSG2100PF, RSG2200F, RSG2300F, RSG2300PF, RSG2488F, RS400F, RS416F, RS416PF, RS900F, RS900GF, RS900GPF, and RS940GF RUGGEDCOM switches, provided by Siemens Canada Ltd. (Siemens). It presents the evaluation results, their justifications, and the conformance results.

This Validation Report is intended to assist the end user of this product and any security certification Agent for that end user in determining the suitability of this Information Technology (IT) product for their environment. End users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this VR, which describes how those security claims were tested and evaluated and any restrictions on the evaluated configuration. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the COACT, Inc. Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America, and was completed in July 2018. The information in this report is largely derived from the associated test reports, all written by COACT, Inc. The evaluation team determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements set forth in the collaborative Protection Profile for Network Devices Version 2.0 + Errata 20180314 (CPP_ND_V2.0E).

The Target of Evaluation (TOE) is identified as the RUGGEDCOM Rugged Operating System (ROS) 4.2.2.F running on the M2100F, M2200F, M969F, RSG2100F, RSG2100PF, RSG2200F, RSG2300F, RSG2300PF, RSG2488F, RS400F, RS416F, RS416PF, RS900F, RS900GF, RS900GPF, and RS940GF RUGGEDCOM switches. The Target of Evaluation identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 4), as interpreted by the assurance activities contained in the CPP_ND_V2.0 + Errata 20180314, hereafter referred to as CPP_ND_V2.0E. This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation test report and the assurance activities report are consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units of the Evaluation Technical Report (ETR) and the Assurance Activity Report (AAR) for the CPP_ND_V2.0E assurance activities. The validation team found that the evaluation showed that the product satisfies all the functional requirements and assurance requirements stated in the Security Target (ST). Therefore, the validation team concludes that the testing laboratory’s findings are accurate, the conclusions justified, and the conformance results are correct. The

conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the Siemens RUGGEDCOM Rugged Operating System (ROS) v4.2.2.F Security Target and analysis performed by the Validation Team.

2. Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) in accordance with the National Voluntary Laboratory Assessment Program (NVLAP) accreditation. CCTLs evaluate products against Protection Profiles containing Assurance Activities, which are interpretations of the Common Evaluation Methodology (CEM) work units specific to the technology described by the PP.

The NIAP Validation Body assigns validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliant List (PCL).

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1 - Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Siemens RUGGEDCOM Rugged Operating System (ROS) v4.2.2.F running on the M2100F, M2200F, M969F, RSG2100F, RSG2100PF, RSG2200F, RSG2300F, RSG2300PF, RSG2488F, RS400F, RS416F, RS416PF, RS900F, RS900GF, RS900GPF, and RS940GF RUGGEDCOM switches
Protection Profile	collaborative Protection Profile for Network Devices, Version 2.0 + Errata 20180314 (CPP_ND_V2.0E)
Security Target	Siemens RUGGEDCOM Rugged Operating System (ROS) v4.2.2.F Security Target, Version 1.3, August 13, 2018

Item	Identifier
Evaluation Technical Report	Siemens RUGGEDCOM Rugged Operating System (ROS) v4.2.2.F Evaluation Technical Report, August 13, 2018.
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 4
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Siemens Canada, Ltd.
Developer	Siemens Canada, Ltd.
Common Criteria Testing Lab (CCTL)	COACT, Inc. Columbia, MD
CCEVS Validators	Jerome F. Myers, Ph.D., The Aerospace Corporation James Donndelinger, The Aerospace Corporation

3. Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

3.1 TOE Introduction

The TOE is a hardware and software TOE consisting of the RUGGEDCOM ROS v4.2.2.F running on the M2100F, M2200F, M969F, RSG2100F, RSG2100PF, RSG2200F, RSG2300F, RSG2300PF, RSG2488F, RS400F, RS416F, RS416PF, RS900F, RS900GF, RS900GPF, and RS940GF RUGGEDCOM switches. The purpose of the TOE is to provide Ethernet switching capabilities in a ruggedized enclosure for customer networks in virtually any environment.

RUGGEDCOM ROS may be deployed on any of the RUGGEDCOM switches mentioned in the TOE above and listed in the "Physical Boundaries" section below. The RUGGEDCOM switches are highly configurable and can be customized with a number of different line module and power supply combinations. Customers choose a configuration that suits the targeted network and Siemens assembles the RUGGEDCOM switches according to the specific configuration. The RUGGEDCOM switches are able to operate in the most adverse conditions and are primarily deployed in power distribution, refineries, or traffic control systems.

These RUGGEDCOM switches are designed specifically to withstand harsh environmental conditions including temperature and humidity extremes, shock, vibration, and electromagnetic interference.

3.2 Physical Boundaries

The physical scope and the physical boundary of the TOE is composed of both the RUGGEDCOM switch hardware and the RUGGEDCOM ROS v4.2.2.F software. For the evaluated configuration, TOE software (ROS v4.2.2.F) was installed and run in the TOE hardware configurations shown in the Table 2 below. The line models on each switch model are configurable and the tested configurations provide a sample of possible configurations. The line modules provide 10/100/1000BaseTX Ethernet, serial, and fiber interfaces that are used to send and receive user data. The line modules provide nothing more than the physical interface.

Table 2 - TOE Models Tested Configuration

Model	HW ID/CPU/Description	Line Card Configuration
M2100F	RSG2100v2 NXP ColdFire MCF5272 M2100FIPS-CC	2x 10FL – Multimode, 850nm, ST, 2km
		2x 100FX – Multimode, 1300nm, ST, 2km
		2x 100FX – Singlemode, 1310nm, ST, 20km
		2x 10/100TX – Micro-D
RSG2100F	RSG2100v2 NXP ColdFire MCF5272 RSG2100FIPS-CC	2x 10/100TX – RJ45
		2x 10FL – Multimode, 850nm, ST, 2km
		2x 100FX – Multimode, 1300nm, ST, 2km
		2x 100FX – Singlemode, 1310nm, LC, 90km
		2x 10/100TX – Micro-D
		2x 10/100/1000TX – RJ45
		1x 1000SX – Multimode, 850nm, LC, 500m
RSG2100PF	RSG2100v2 NXP ColdFire MCF5272 RSG2100PFIPS-CC	2x 10/100TX – RJ45
		2x 100FX – Multimode, 1300nm, ST, 2km
		2x 100FX – Multimode, 1300nm, MTRJ, 2km
		2x 100FX – Singlemode, 1310nm, SC, 90km
		2x 1000LX – Singlemode, 1310nm, LC, 25km
		1x 1000SX – Multimode, 850nm, LC, 500m
		2x 10/100TX – Micro-D
		2x 10/100TX – Micro-D
M2200F	RSG2200 NXP ColdFire MCF5272 M2200FIPS-CC	2x 10/100/1000TX – Micro-D
		2x 1000SX – Multimode, 850nm, LC, 500m
		2x 1000LX – Singlemode, 1310nm, LC, 25km
		2x 10/100/1000TX – Micro-D
		2x 10/100/1000TX – Micro-D
RSG2200F	RSG2200 NXP ColdFire MCF5272	2x 10/100/1000TX – RJ45
		2x 1000SX – Multimode, 850nm, LC, 500m

	RSG2200FIPS-CC	2x 1000LX – Singlemode, 1310nm, LC, 25km
		2x 1000SX – Multimode, 850nm, LC, 500m
		1x 100FX – Multimode, 1300nm, MTRJ, 2km
RSG2300F	RSG2300 NXP ColdFire MCF5272 RSG2300FIPS-CC	2x 10/100TX – RJ45
		2x 100FX – Multimode, 1300nm, MTRJ, 2km
		2x 1000SX – Multimode, 850nm, LC, 500m
		2x 10/100/1000TX – RJ45
RSG2300PF	RSG2300 NXP ColdFire MCF5272 RSG2300PFIPS-CC	2x 10/100TX – RJ45
		2x 10/100TX – RJ45
		2x 1000SX – Multimode, 850nm, LC, 500m
		2x 100FX – Multimode, 1300nm, MTRJ, 2km
RSG2488F	RSG2488v2 NXP PowerQUICC MPC8308 RSG2488FIPS-CC	4x 10/100/1000TX – RJ45
		4x 10/100/1000TX – M12 X-Coded
		4x 1000SX – Multimode, 850nm, LC, 500m
		4x 1000SX – Multimode, 850nm, LC, 500m
		4x 1000LX – Singlemode, 1310nm, LC, 25km
		1x Precision Time Protocol (PTP) Module
		2x 10/100/1000TX – RJ45
		2x 10/100/1000TX – M12 X-Coded
RS416F	RSG416v2 NXP ColdFire MCF5272 RS416FIPS-CC	4x 10FL – Multimode, 850nm, ST, 2km
		4x RS232/RS422/RS485 & IRIG-B – DB9
		4x RS232/RS422/RS485 & IRIG-B – RJ45
		2x 10/100TX – RJ45
		1x IRIG-B in – BNC
		1x IRIG-B out – BNC (Slot 5 only)
RS416PF	RS416v2 NXP ColdFire MCF5272 RS416PFIPS-CC	4x 10FL – Multimode, 850nm, ST, 2km
		4x RS232/RS422/RS485 & IRIG-B – DB9
		4x RS232/RS422/RS485 & IRIG-B – RJ45
		1x IRIG-B in – BNC
		1x IRIG-B out – BNC (Slot 5 only)
		2x 10/100TX – RJ45
RS400F	RS400 (40-00-0010 Rev C1) NXP ColdFire MCF5272 RS400FIPS-CC	1x 100FX – Multimode, 1310nm, LC, 2km
		1x 100FX – Singlemode, 1300nm, LC, 20km
		4x RS232/RS422/RS485 – DB9
RS940GF	RS940G (40-00-0097-000 Rev A) NXP ColdFire MCF5272 RS940GFIPS-CC	2x 1000SX – Multimode, 850nm, LC, 500m

RS900GF	RS900Gv2 NXP ColdFire MCF5272 RS900FIPS-CC	2x 1000LX – Singlemode, 1310nm, LC, 25km
RS900GPF	RS900GP NXP ColdFire MCF5272 RS900GFIPS-CC	2x 1000LX – Singlemode, 1310nm, SC, 25km
RS900F	RS900v3, Fiber NXP ColdFire MCF5272 RS900FIPS-CC	2x 100FX – Multimode, 1300nm, ST, 2km
		1x 100FX – Singlemode, 1310nm, ST, 20km
		1x 100FX – Multimode, 1300nm, SC, 2k
M969F	RS969 (v2, 40-00-0090) NXP ColdFire MCF5272 M969FIPS-CC	2x 1000SX – Multimode, 850nm, LC, 500m

4. Security Policy

This section summarizes the security functionality of the TOE.

4.1 Security Audit

The TOE generates audit records for security-relevant actions of the authorized administrators accessing the TOE via the terminal-based menu and web interface. The TOE records the identity of the administrator responsible for the log event, where applicable. To remotely and securely backup the audit logs, an Administrator can configure the syslog server to call into the TOE and request audit log files be printed to the syslog server over an SSH connection. The connection to the audit server is secured using SSH. When logs are filled, the TOE overwrites in two possible ways: the oldest log record can be overwritten with the new log record or the oldest log file can be overwritten with the new log file.

4.2 Cryptographic Support

The TOE algorithms were validated through the Cryptographic Algorithm Validation Program (CAVP). The TOE contains cryptographic support that provides key generation, random bit generation, encryption/decryption, digital signature and secure hashing, key-hashing, and key establishment features in support of higher level cryptographic protocols including SSH and TLS.

4.3 Identification and Authentication

The TOE provides functionality that requires administrators to verify their claimed identity. The TOE ensures that only authorized administrators can gain access to configuration and management settings. Administrators can only view the access banner prior to authenticating with a valid user name and password. The TOE requires administrators to use strong passwords. The TOE provides no feedback to Administrators when they are entering their passwords at the login prompt of the terminal-based menu for both direct serial and remote SSH connections. Administrators using password-based authentication are locked out after a configurable number of unsuccessful authentication attempts and must wait a configurable period of time before they are unlocked. The TOE can present a certificate to authenticate to external entities and this certificate and the

trust anchor certificate are stored within a truststore. Certificate revocation status is verified on certificates uploaded to the TOE using an external Online Certificate Status Protocol (OCSP) server.

4.4 Security Management

The TOE provides a web interface and a terminal-based menu for administrators to manage the security functions, configuration, and other features of the TOE. The security management function specifies user roles with defined access for the management of the TOE components. Updating the TOE, modifying the configuration file, configuring the access banner, setting the inactivity timeout, configuring authentication failure parameters, configuring time and re-enabling the Administrator account are all functions restricted to the Security Administrator.

4.5 Protection of the TSF

The TOE invokes a set of self-tests each time the TOE is powered on to ensure that the TSF operates correctly. The TOE also provides a reliable timestamp for its own use. An Administrator can manually set the time for the TOE. A digital signature using an RSA public key is used to verify all software updates that are applied to the TOE. The TOE prevents an administrator from reading the keys stored in the TOE. Passwords are stored in obfuscated form to prevent them from being read in plaintext.

4.6 TOE Access

The TOE terminates local and remote management sessions after an administrator-configurable time period of inactivity. The TOE also provides administrator's the capability to manually terminate the session prior to the inactivity timeout. After an administrator's session is terminated, the administrator must log in again to regain access to TOE functionality. A login banner is displayed at the login screen of the web interface and prior to authentication over the terminal-based menu.

4.7 Trusted Path / Channels

The cryptographic functionality of the TOE provides the TOE the ability to create trusted paths and trusted channels. The TOE implements a trusted channel using SSH between itself and a remote server in order to protect the audit logs as they are being sent. Additionally, the TOE provides trusted paths between administrators and the web interface via HTTPS and the terminal-based menu via SSH. The management communication channels between the TOE and a remote entity are distinct from network data communication channels and provide mutual identification and authentication. In addition, the communications are protected from modification and disclosure.

5. Assumptions

The Security Problem Definition, including the assumptions, may be found in the following document:

- collaborative Protection Profile for Network Devices, Version 2.0 + Errata 20180314

That information has not been reproduced here and the CPP_ND_V2.0E should be consulted if there is interest in that material.

6. Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made with a certain level of assurance (the assurance activities specified in CPP_NDV2.0E and performed by the evaluation team).
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The functionality evaluated is scoped strictly to the security functional requirements specified in the CPP_ND_V2.0E and applicable Technical Decisions. Any additional security or non-security related functional capabilities of the product (defined in Section 1.5.3 of the Security Target) were not covered by this evaluation.
    - Specifically, the following product features were not in the scope of evaluation and thus were not tested:
        - Virtual Local Area Network configuration
        - Port configuration
        - Broadcast Storm filtering
        - Quality of Service based on part, tag, MAC16, or IP type of service
        - Multiple Spanning Tree Protocol
        - Rapid Spanning Tree Protocol
        - Enhanced Rapid Spanning Tree Protocol
    - The following services are present in the TOE but are excluded from use in the evaluated configuration:
        - RADIUS
        - TACACS+
        - RSH

- Telnet
- TFTP
- ModBus Management
- Remote Syslog
- Management connections over SNMP v1, v2, and v3
- Management via HTTP
- Network Time Protocol (NTP) time synchronisation and service
- RUGGEDCOM Discovery Protocol (RCDP)
- IP Forwarding.

7. Documentation

The following documents were used as evidence for the evaluation of the Siemens RUGGEDCOM Rugged Operating System (ROS) v4.2.2.F:

- Siemens RUGGEDCOM Rugged Operating System (ROS) v4.2.2.F Guidance Documentation Supplement, 08/2018
- FAQ - "How to Transfer Secure Audit Logs" (referenced in Guidance Documentation Supplement)

In addition to these documents, Siemens general installation and user guidance documents specific to each device (or group of devices) included in the TOE are listed in section 1.1 of the Guidance Documentation Supplement and were used to install and configure the TOE in the Common Criteria-evaluated configuration. These documents can be downloaded from the vendor website. The CC Guidance Documentation Supplement provides clarifications and changes to the Siemens general product documentation and should be used as the guiding document for the installation and administration of the TOE in the CC-evaluated configuration. The Siemens general installation and user guidance documentation should be referred to and followed only as directed within the CC Guidance Documentation Supplement and for the performance of the AGD assurance activities as described in the AAR. Note that only sections referenced by the CC Guidance Documentation Supplement and/or used during the evaluation of the AGD assurance activities (as described in the AAR), are covered by the evaluation.

The Security Target used is:

- Siemens RUGGEDCOM Rugged Operating System (ROS) v4.2.2.F Security Target, Version 1.3, August 13, 2018

8. IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information summarized in the publicly available Assurance Activity Report Siemens RUGGEDCOM Rugged Operating System (ROS) v4.2.2.F.

8.1 Developer Testing

No evidence of developer testing is required in the assurance activities for this product.

8.2 Evaluation Team Testing

Testing was performed at COACT CC Testing Lab located at: COACT, Inc., 9140 Guilford Road, Suite N Columbia, MD 21046.

The evaluation team verified the product according the Siemens RUGGEDCOM Rugged Operating System (ROS) v4.2.2.F Guidance Documentation Supplement and performed the tests and documentation analysis as specified in the CPP_ND_V2.0E and its Supporting Document (SD).

8.2.1 TOE Test Configuration

The following diagram provides a visual depiction the TOE test configuration.

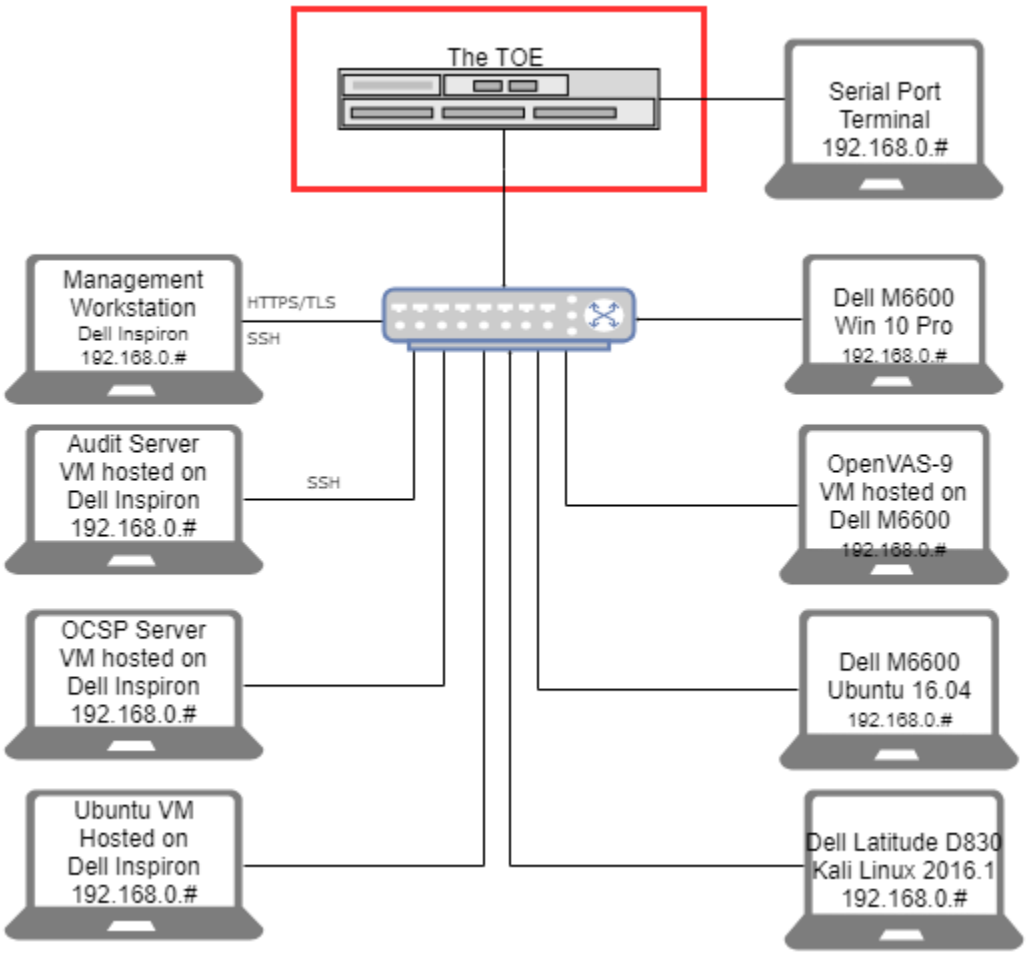

Figure 1 - The TOE Test Configuration

The TOE's connection to a management client accessing the GUI is protected by TLS. The TOE's connection to an audit server or a management client accessing the CLI is protected by SSH.

- The TOE:
    a. Siemens ROS switches (see section "Physical Boundaries" section above)
    b. RUGGEDCOM Rugged Operating System (ROS) v4.2.2.F
- Management Workstation is a Dell workstation running MS Windows 10 Pro with IE 11 (used for the serial port connection also)
- Audit Server – an Ubuntu virtual box hosted on the Management Workstation machine
- OCSP Server – an Ubuntu virtual box hosted on the Management Workstation machine used to generate X.509 Certificates and run the OCSP responder.
- Ubuntu 16.04 – a virtual box hosted on the Management Workstation machine to run the COACT tool.
- Dell Latitude D830 with Kali Linux 2016.1 - used for packet capture
- DELL Precision M6600 with Win 10 Pro used for pen-testing
- DELL Precision M6600 with Ubuntu 16.04 to run the COACT tool for pen-testing
- OpenVAS-9 – Virtual Box hosted on DELL Precision M6600 Win 10 Pro

8.2.2 Test Tools

- Windows 10 Pro
- Wireshark 2.2.4/2.4.6
- OpenSSL 1.0.0.54/1.0.2g
- VirtualBox 5.1.28r117968/v5.2.10
- Firefox Developer Edition 58.0
- Firefox v1.0
- NMAP v7.31/v7.7
- Tera Term 4.92/4.93
- PuTTY Release 0.67
- BitVise SSH Client 7.29
- HxD Hex Editor 1.7.7.0
- WinPcap 4.1.3
- Rlogin SSH Client 4.22.2
- Ubuntu xenial 16.04.4 LTS
- autossh 1.4e
- OpenSSH_7.2p2
- Python 2.7
- "COACT Protocol Implementation Testing Scripts" (CPITS)
- Kali Linux 2016.1
- minicom version 2.7
- OWASP ZAP v.2.7.0
- GSM Community Edition Version 4.1.7 with OpenVAS-9

9. Evaluated Configuration

The TOE is a hardware and software TOE. For the evaluated configuration, the TOE software (RUGGEDCOM ROS v4.2.2.F) must be installed and run on one of the RUGGEDCOM switches listed in the "Physical Boundaries" section above.

The TOE must be configured in the CC evaluated configuration by following the steps described in the RUGGEDCOM ROS v4.2.2.F User Guide (using the corresponding document specific to each model configured and evaluated) and the Siemens RUGGEDCOM ROS Guidance Supplement document.

10. Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR and the Assurance Activities Report (AAR). The reader of this document can assume that all assurance activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 4 and CEM version 3.1 rev 4. The evaluation determined the Siemens RUGGEDCOM Rugged Operating System (ROS) v4.2.2.F TOE to be Part 2 extended, and meets the SARs contained the CPP_ND_V2.0E.

10.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Siemens RUGGEDCOM Rugged Operating System (ROS) v4.2.2.F products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validators reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

10.2 Evaluation of the Development (ADV)

The evaluation team applied each ADV CEM work unit and updated them with corresponding Assurance Activity defined in CPP_ND_V2.0E and its Supporting Document. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target and Guidance documents.

The validators reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

10.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally, the evaluator performed additional assurance activities specified in the CPP_ND_V2.0E and its Supporting Document.

The validators reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

10.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work unit. The evaluation team found that the TOE was identified.

The validators reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

10.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the assurance activities in the CPP_ND_V2.0E and its Supporting Document and recorded the results in a Detailed Test Report (proprietary), summarized in the AAR.

The validators reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

10.6 Vulnerability Assessment Activity (AVA)

The evaluation team applied each AVA CEM work unit updated with respective Assurance Activities defined in the Supporting Document as required by the CPP_ND_V2.0E. The evaluation team performed a public search for vulnerabilities and performed vulnerability testing. The information for the public vulnerability sources searched, keywords used as searching criteria and results and the analysis of these searches are provided in section 3.1 of the Assurance Activity Report.

The validators reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM and the SD, and that the conclusion reached by the evaluation team was justified.

10.7 Summary of the Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's test activities also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the Assurance Activities in the CPP_ND_V2.0E and correctly verified that the product meets the claims in the ST.

11. Validator Comments / Recommendations

The validators did not have any specific additional comments or recommendations.

12. Annexes

Not applicable

13. Security Target

Siemens RUGGEDCOM Rugged Operating System (ROS) v4.2.2.F Security Target, Version 1.1, July 13, 2018.

14. Glossary

The following definitions are used throughout this document:

Common Criteria Testing Laboratory (CCTL). An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.

Conformance. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.

Evaluation. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology as interpreted by the supplemental guidance in the NDPP Assurance Activities to determine whether or not the claims made are justified.

Evaluation Evidence. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.

Target of Evaluation (TOE). A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.

Validation. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.

Validation Body. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

15. Bibliography

The Validation Team used the following documents to produce this Validation Report:

1. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 4, dated: September 2012.
2. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 4, dated: September 2012.
3. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 4, dated: September 2012.
4. *Common Methodology for Information Technology Security Evaluation: Evaluation Methodology*, Version 3.1, Revision 4, dated: September 2012.
5. *collaborative Protection Profile for Network Devices*, Version 2.0 + Errata 20180314 (CPP_ND_V2.0E).
6. *Siemens RUGGEDCOM Rugged Operating System (ROS) v4.2.2.F Security Target, Version 1.3, August 13, 2018.*
7. *Siemens RUGGEDCOM Rugged Operating System (ROS) v4.2.2.F Evaluation Technical Report (ETR), August 13, 2018.*
8. *Detailed Test Report* for *Siemens RUGGEDCOM Rugged Operating System v4.2.2.F* (DTR), August 13, 2018.
9. *Assurance Activity Report for Siemens RUGGEDCOM Rugged Operating System v4.2.2.F* (AAR), August 13, 2018.
10. *Vulnerability Analysis Report for Siemens RUGGEDCOM Rugged Operating System v4.2.2.F,* August 13, 2018.
11. *Siemens Canada Ltd. RUGGEDCOM Rugged Operating System v4.2.2.F Guidance Documentation Supplement* (AGD), 08/2018.
    a. *User Guide (referenced in the AGD, can be downloaded from the vendor website)*
    b. *Installation Guide (referenced in the AGD, can be downloaded from the vendor website)*
12. *FAQ - "How to Implement Secure, Unattended Logging in ROS", V 1.0, 05/2018*

End of Document