National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for

Hewlett Packard Enterprise MSR1000 Series, MSR2000 Series, MSR3000 Series and MSR4000 Series Routers

Report Number: CCEVS-VR-VID10670-2016
Dated: March 4, 2016
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

Table of Contents

List of Tables

List of Figures

1 Executive Summary

This 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 in their environment. End-users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated and tested and any restrictions on the evaluated configuration. Prospective users should read carefully the Assumptions and Clarification of Scope in Section 4 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation Hewlett Packard Enterprise MSR Routers 1k-4k with Comware V7.1.059, Release 0305. It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and as documented in the ST.

The evaluation of the Hewlett Packard Enterprise MSR Routers 1k-4k with Comware V7.1.059, Release 0305 was performed by Leidos (formerly Science Applications International Corporation (SAIC)) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, in the United States and was completed in February 2016. The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1, revision 4 and assurance activities specified in Protection Profile for Network Devices, Version 1.1, 8 June 2012 and Security Requirements as amended by Errata #3 dated 3 November 2014, and includes the additional optional SFRs: FCS_IPSEC_EXT.1; FCS_SSH_EXT.1; and FIA_PSK_EXT.1.

The evaluation was consistent with NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap-ccevs.org).

The Leidos evaluation team determined that the Hewlett Packard Enterprise MSR Routers 1k-4k comprising a common software code base of Comware V7.1.059, Release 0305 is conformant to the claimed Protection Profile (PP) and, when installed, configured and operated as specified in the evaluated guidance documentation, satisfies all of the security functional requirements stated in the ST. The information in this VR is largely derived from the Assurance Activities Report (AAR) and the associated proprietary test report produced by the Leidos evaluation team.

The TOE is a hardware and software solution that consists of the Comware V7.1.059, Release 0305 software running on one or more of the Hewlett Packard Enterprise appliances listed below:

Product Series	**Specific Devices**
HP MSR1000	HP MSR1002-4 AC Router ((JG875A) HP MSR1003-8S AC Router (JH060A)
HP MSR2000	HP MSR2003 AC Router (JG411A) HP MSR2004-24 AC Router (JG734A) HP MSR2004-48 Router (JG735A)
HP MSR3000	HP MSR3012 AC Router (JG409A) HP MSR3012 DC Router (JG410A) HP MSR3024 AC Router ((JG406A) HP MSR3024 DC Router (JG407A)

Product Series	Specific Devices
	HP MSR3024 PoE Router (JG408A) HP MSR3044 Router (JG405A) HP MSR3064 Router (JG404A)
HP MSR4000	HP MSR 4060 Router Chassis with HP MSR4000 MPU-100 Main Processing Unit (JG403A) HP MSR 4080 Router Chassis with HP MSR4000 MPU-100 Main Processing Unit (JG402A) Note: Each MSR4000 product series must also have one of the following Service Processing Units : • HP MSR4000 SPU-100 Service Processing Unit (JG413A); • HP MSR4000 SPU-200 Service Processing Unit (JG414A); or • HP MSR4000 SPU-300 Service Processing Unit (JG670A).

The network on which it resides is considered part of the operational environment.

The validation team examined evaluation evidence, provided guidance on technical issues and evaluation processes, and reviewed the evaluation results produced by the evaluation team. The validation team found that the evaluation results showed that all assurance activities specified in the claimed PPs had been completed successfully and that the product satisfies all of the security functional and assurance requirements stated in the 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.

Table 1: Evaluation Details

Item	Identifier

Item	Identifier
Evaluated Product	Hewlett Packard Enterprise MSR 1000, 2000, 3000, and 4000 Series Routers with Comware V7.1.059, Release 0305 HP MSR1002-4 AC Router ((JG875A) HP MSR1003-8S AC Router (JH060A) HP MSR2003 AC Router (JG411A) HP MSR2004-24 AC Router (JG734A) HP MSR2004-48 Router (JG735A) HP MSR3012 AC Router (JG409A) HP MSR3012 DC Router (JG410A) HP MSR3024 AC Router ((JG406A) HP MSR3024 DC Router (JG407A) HP MSR3024 PoE Router (JG408A) HP MSR3044 Router (JG405A) HP MSR3064 Router (JG404A) HP MSR 4060 Router Chassis with HP MSR4000 MPU-100 Main Processing Unit (JG403A) HP MSR 4080 Router Chassis with HP MSR4000 MPU-100 Main Processing Unit (JG402A) Note: Each MSR4000 product series must also have one of the following Service Processing Units : • HP MSR4000 SPU-100 Service Processing Unit (JG413A); • HP MSR4000 SPU-200 Service Processing Unit (JG414A); or • HP MSR4000 SPU-300 Service Processing Unit (JG670A).
Sponsor & Developer	Hewlett Packard Enterprise 11445 Compaq Center Drive West Houston, Texas 77070 United States
CCTL	Leidos (formerly SAIC) Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Completion Date	February 2016
CC	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012
Interpretations	There were no applicable interpretations used for this evaluation.

Item	Identifier
CEM	Common Methodology for Information Technology Security Evaluation: Version 3.1, Revision 4, September 2012
PP	Protection Profile for Network Devices, Version 1.1, 8 June 2012 and Security Requirements as amended by Errata #3 dated 3 November 2014, and including the following optional SFRs: FCS_IPSEC_EXT.1; FCS_SSH_EXT.1; and FIA_PSK_EXT.1.
Disclaimer	The information contained in this Validation Report is not an endorsement either expressed or implied of the Hewlett Packard Enterprise MSR 1000, 2000, 3000, and 4000 Series Routers with Comware V7.1.059, Release 0305 HP MSR1002-4 AC Router ((JG875A) HP MSR1003-8S AC Router (JH060A) HP MSR2003 AC Router (JG411A) HP MSR2004-24 AC Router (JG734A) HP MSR2004-48 Router (JG735A) HP MSR3012 AC Router (JG409A) HP MSR3012 DC Router (JG410A) HP MSR3024 AC Router ((JG406A) HP MSR3024 DC Router (JG407A) HP MSR3024 PoE Router (JG408A) HP MSR3044 Router (JG405A) HP MSR3064 Router (JG404A) HP MSR 4060 Router Chassis with HP MSR4000 MPU-100 Main Processing Unit (JG403A) HP MSR 4080 Router Chassis with HP MSR4000 MPU-100 Main Processing Unit (JG402A) Note: Each MSR4000 product series must also have one of the following Service Processing Units : • HP MSR4000 SPU-100 Service Processing Unit (JG413A); • HP MSR4000 SPU-200 Service Processing Unit (JG414A); or • HP MSR4000 SPU-300 Service Processing Unit (JG670A).
Evaluation Personnel	Greg Beaver Cody Cummins Tony Apted
Validation Personnel	Jerome Myers Ken Stutterheim Meredith Hennan

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 National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

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).

The following table identifies the evaluated Security Target and TOE.

Table 2: ST and TOE Identification

Name	Description
ST Title	Hewlett Packard Enterprise MSR Routers 1k-4k Security Target
ST Version	1.0
Publication Date	February 16, 2016
Vendor	Hewlett Packard Enterprise
ST Author	Leidos (formerly SAIC)
TOE Reference	The Hewlett Packard Enterprise MSR 1000, 2000, 3000, and 4000 Series Routers with Comware V7.1.059, Release 0305: HP MSR1002-4 AC Router ((JG875A) HP MSR1003-8S AC Router (JH060A) HP MSR2003 AC Router (JG411A) HP MSR2004-24 AC Router (JG734A) HP MSR2004-48 Router (JG735A) HP MSR3012 AC Router (JG409A) HP MSR3012 DC Router (JG410A) HP MSR3024 AC Router ((JG406A) HP MSR3024 DC Router (JG407A) HP MSR3024 PoE Router (JG408A) HP MSR3044 Router (JG405A) HP MSR3064 Router (JG404A) HP MSR 4060 Router Chassis with HP MSR4000 MPU-100 Main Processing Unit (JG403A) HP MSR 4080 Router Chassis with HP MSR4000 MPU-100 Main Processing Unit (JG402A) Note: Each MSR4000 product series must also have one of the following Service Processing Units : • HP MSR4000 SPU-100 Service Processing Unit (JG413A); • HP MSR4000 SPU-200 Service Processing Unit (JG414A); or

	• HP MSR4000 SPU-300 Service Processing Unit (JG670A).
TOE Software Version	Comware V7.1.059, Release 0305
Keywords	Gigabit Ethernet Router, Network Layer 2, Network Layer 3

2.1 Threats

The ST references the Protection Profile for Network Devices to identify the following threats that the TOE and its operational environment are intended to counter:

- An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
- Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
- A user may gain unauthorized access to the TOE data and TOE executable code. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.
- A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.
- Malicious remote users or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated.
- User data may be inadvertently sent to a destination not intended by the original sender.

2.2 Organizational Security Policies

The ST references the Protection Profile for Network Devices to identify following organizational security policy that the TOE and its operational environment are intended to fulfill:

- The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

3 Architectural Information

The various routers comprising the TOE share a common software code base, named Comware. Comware is special purpose appliance system software that supports the implementation of a wide array of networking technology. The underlying architecture in the evaluated configuration is Linux.

Comware V7.1 comprises four planes: management plane, control plane, data plane, and infrastructure plane:

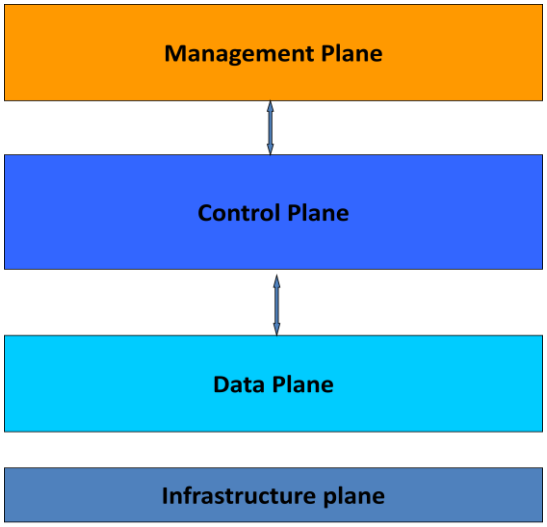

Figure 1 Comware V7.1 Architecture

- ***Infrastructure plane*** – The infrastructure plane provides basic Linux services and Comware support functions. Basic Linux services comprise basic Linux functions, C language library functions, data structure operations, and standard algorithms. Comware support functions provide software and service infrastructures for Comware processes, including all basic functions.
- ***Data plane*** – The data plane provides data forwarding for local packets and received IPv4 and IPv6 packets at different layers.
- ***Control plane*** – The control plane comprises all routing, signaling, and control protocols, such as MPLS, OSPF, and security control protocols. It generates forwarding tables for the data plane.
- ***Management plane*** – The management plane provides a management interface for operators to configure, monitor, and manage Comware V7.1. The management interface comprises a CLI accessed using Secure Shell (SSH).

From a security perspective, the TOE implements NIST-validated cryptographic algorithms that support the IPsec and SSH protocols as well as digital signature services that support the secure update capabilities of the TOE.

The various TOE devices include the same security functions. The salient differences between the devices are the available ports and port adapters primarily representing differences in numbers, types, and speeds of available network connections.

4 Assumptions

The ST references the Protection Profile for Network Devices to identify following assumptions about the use of the product:

- It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
- Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
- TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

4.1 Clarification of Scope

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

1. 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 the claimed PPs and performed by the evaluation team).
2. This evaluation covers only the specific device models and software version identified in this document, and not any earlier or later versions released or in process.
3. The evaluation of security functionality of the product was limited to the functionality specified in the claimed NDPP. Any additional security related functional capabilities of the product were not covered by this evaluation.
4. 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.
5. The following specific product capabilities are excluded from use in the evaluated configuration:
    a. Non-FIPS 140-2 mode of operation—this mode of operation allows cryptographic operations that are not FIPS-approved
6. The TOE can be configured to rely on and utilize a number of other components in its operational environment:
    a. Syslog server—to receive audit records when the TOE is configured to deliver them to an external log server.
    b. RADIUS and TACACS servers—the TOE can be configured to use external authentication servers.
    c. Management Workstation—the TOE supports remote access to the CLI over SSHv2. As such, an administrator requires an SSHv2 client to access the CLI remotely.

5 Security Policy

The TOE enforces the following security policies as described in the ST.

5.1 Security Audit

The TOE is able to generate logs of security relevant events including the events specified in NDPP. The TOE can be configured to store the logs locally so they can be accessed by an administrator or alternately to send the logs to a designated external log server.

5.2 Cryptographic Support

The TOE includes NIST-validated cryptographic mechanisms that provide key management, random bit generation, encryption/decryption, digital signature and secure hashing and key-hashing features in support of higher level cryptographic protocols, including IPsec and SSHv2. Note that in the evaluated configuration, the TOE must be configured in FIPS mode.

5.3 User Data Protection

The TOE performs network switching and routing functions, passing network traffic among its various physical and logical network connections. While implementing applicable network protocols associated with network traffic forwarding, the TOE employs mechanisms to ensure that it does not inadvertently reuse data found in network traffic.

5.4 Identification and Authentication

The TOE requires administrators to be successfully identified and authenticated before they can access any security management functions available in the TOE. The TOE offers both a locally connected console and a network accessible interface (SSHv2) for interactive administrator sessions.

The TOE supports on device definition of administrators with usernames and passwords. Additionally, the TOE can be configured to utilize the services of trusted RADIUS and TACACS+ servers in the operational environment to support centralized user administration. The TOE supports the use of text-based pre-shared keys for IKE peer authentication.

5.5 Security Management

The TOE provides Command Line (CLI) commands to access the security management functions. Security management commands are limited to administrators and are available only after they have provided acceptable user identification and authentication data to the TOE.

5.6 Protection of the TSF

The TOE implements features to protect itself to ensure the reliability and integrity of its security features.

It protects data such as stored passwords and cryptographic keys so that they are not accessible even by an administrator. It also provides its own timing mechanism to ensure that reliable time information is available (for example, for log accountability).

The TOE uses cryptographic means to protect communication with remote administrators. When the TOE is configured to use the services of a Syslog server or authentication servers in the operational environment, the communication between the TOE and the operational environment component is protected using encryption.

The TOE includes functions to perform self-tests so that it might detect when it is failing. It also includes mechanisms so that the TOE itself can be updated while ensuring that the updates will not introduce malicious or other unexpected changes in the TOE.

5.7 TOE Access

The TOE can be configured to display an informative banner that will appear prior to authentication when accessing the TOE via the console or SSH interfaces. The TOE subsequently will enforce an administrator-defined inactivity timeout value, after which the inactive session will be terminated.

5.8 Trusted Path/Channels

The TOE protects interactive communication with administrators using SSHv2 for CLI access. Using SSHv2, both integrity and disclosure protection are ensured.

The TOE protects communication with network peers, such as audit and authentication servers, using IPsec connections to prevent unintended disclosure or modification of data.

6 Documentation

There are numerous documents that provide information and guidance for the deployment of the TOE. Only those documents that were used to place the TOE into its evaluated configuration are considered to be part of the evaluated TOE. Any additional customer documentation delivered with the TOE or made available through electronic downloads should not be relied upon for using the TOE in its evaluated configuration.

In particular, there are four Common Criteria specific guides that reference the security-related guidance material for all products evaluated and were used in the evaluation:

- Preparative Procedures for CC NDPP Evaluated Hewlett Packard Enterprise MSR1000, MSR2000, MSR3000 and MSR4000 router series based on Comware V7.1, version 1.01, February 16, 2016
- Command Reference for CC Supplement, Revision 1.05, 1/22/2016
- Configuration Guide for CC Supplement, Revision 1.6, 1/22/2016
- Comware V7 System Log Messages Reference, Revision 1.0, 2014-04-21

The links in the table below for each series can be used to find the full set of documentation for each of the evaluated router series. Note that only the documents listed above were examined during the course of the evaluation, and are the approved documents for configuring and using the TOE in its evaluated configuration.

Product Family	Link to Series Documentation
MSR1000 Series	http://h20566.www2.hpe.com/portal/site/hpsc/public/psi/home/?sp4ts.oid=6796027&ac.admitted=1451955288924.125225703.1938120508#manuals
MSR 2000 series	http://h20566.www2.hpe.com/portal/site/hpsc/public/psi/home/?sp4ts.oid=5408894&ac.admitted=1453513446265.125225703.1938120508#manuals
MSR 3000 series	http://h20566.www2.hpe.com/portal/site/hpsc/public/psi/home/?sp4ts.oid=5408895#manuals
MSR 4000 series	http://h20565.www2.hpe.com/portal/site/hpsc/public/kb/search/?sp4ts.oid=5408896

Supporting TOE Guidance Documentation

- Hewlett Packard Enterprise MSR Routers 1k-4k Security Target, Version 1.0, February 16, 2016

7 Independent Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in the following proprietary document that was provided to NIAP:

- Evaluation Team Test Report for Hewlett Packard Enterprise 1K – 4K Routers, Version 1.0, February 16, 2016

as summarized in the publically available document:

- Assurance Activities Report for Hewlett-Packard Company MSR 1000, 2000, 3000, and 4000 Series Routers with Comware 7.1 Version 1.0, 16 February 2016.

The purpose of this activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST for a product claiming conformance to the Protection Profile for Network Devices, Version 1.1, 8 June 2012 and Security Requirements as amended by Errata #3 dated 3 November 2014, and including the following optional SFRs: FCS_IPSEC_EXT.1; FCS_SSH_EXT.1; and FIA_PSK_EXT.1.

The evaluation team devised a Test Plan based on the Testing Assurance Activities specified in the Protection Profile for Network Devices, Version 1.1, 8 June 2012 and Security Requirements as amended by Errata #3 dated 3 November 2014, and including the following optional SFRs: FCS_IPSEC_EXT.1; FCS_SSH_EXT.1; and FIA_PSK_EXT.1.

The Test Plan described how each test activity was to be instantiated within the TOE test environment. The evaluation team executed the tests specified in the Test Plan and documented the results in the team test report listed above and summarized those in the Assurance Activities Report as previously noted.

Independent testing took place at the Leidos facility in Columbia, Maryland from November 10, 2015 – February 1, 2016.

The evaluators received the TOE in the form that normal customers would receive it, installed and configured the TOE in accordance with the provided guidance, and exercised the Team Test Plan on equipment configured in the testing laboratory.

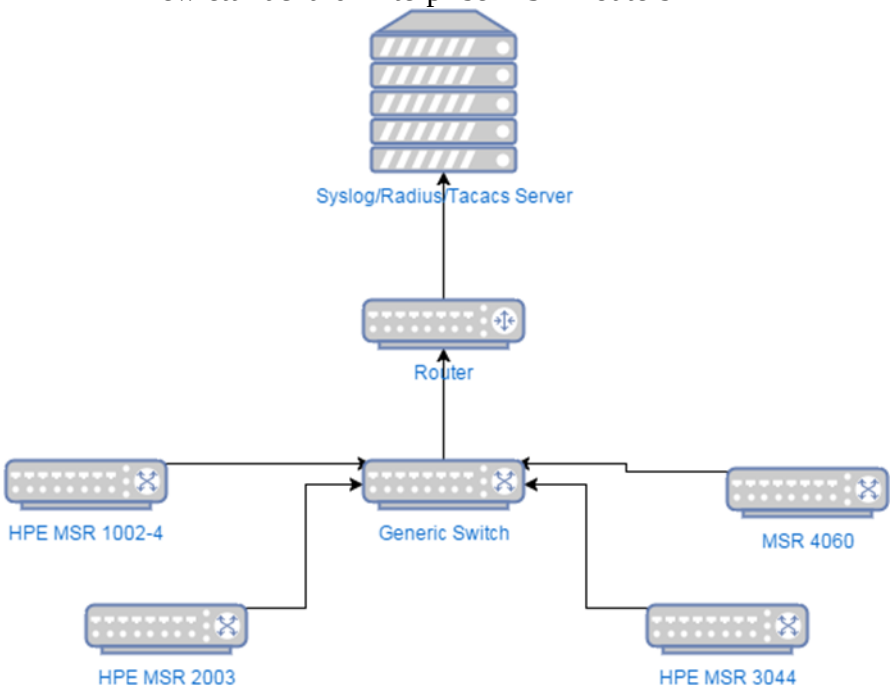

Figure 2 Configuration Used for Testing

As documented in the diagram above, the following hardware and software components were included in the evaluated configuration during testing:

- Hardware
  - HP MSR1002-4 AC Router
  - HP MSR3044 Router
  - HP MSR2003 AC Router
  - HP MSR 4060 Router Chassis with HP MSR4000 MPU-100 Main Processing Unit and the SPU-100 Service Processing Unit
- Software
  - Comware V7.1.059, Release 0305

The following components are not part of the TOE but were included in the testing environment:

- Syslog - 3CDaemon Version 2.0 Revision 10 running on Windows Server 2008
- Syslog - 3CDaemon Version 2.0 Revision 10 running on Windows XP
- RADIUS

The evaluated version of the TOE was installed and configured according to the document: *Preparative Procedures for CC NDPP Evaluated Hewlett Packard Enterprise MSR1000, MSR2000, MSR3000 and MSR4000 Router Series Based on Comware V7.1* as well as the supporting guidance documentation identified in Section 6.

Given the complete set of test results from the test procedures exercised by the evaluators, the testing requirements for the Protection Profile for Network Devices, Version 1.1, 8 June 2012 and Security Requirements as amended by Errata #3 dated 3 November 2014, and includes the additional optional SFRs: FCS_IPSEC_EXT.1; FCS_SSH_EXT.1; and FIA_PSK_EXT.1 are fulfilled.

7.1 Penetration Testing

The evaluation team conducted a limited open source search for vulnerabilities in the product using simple product related search terms via several known vulnerability tracking websites. The open source search did not identify any obvious vulnerabilities applicable to the TOE in its evaluated configuration. The search results and analysis are contained in the *Assurance Activities Report for Hewlett-Packard Company MSR 1000, 2000, 3000, and 4000 Series Routers with Comware 7.1* Version 1.0, 16 February 2016.

8 Results of the Evaluation

The evaluation was conducted based upon the assurance activities specified in Protection Profile for Network Devices, Version 1.1, 8 June 2012 and Security Requirements as amended by Errata #3 dated 3 November 2014, and includes the additional optional SFRs: FCS_IPSEC_EXT.1; FCS_SSH_EXT.1; and FIA_PSK_EXT.1, in conjunction with version 3.1, revision 4 of the CC and the CEM. A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements.

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 claimed PPs, and correctly verified that the product meets the claims in the ST.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by the Leidos CCTL. The security assurance requirements are listed in the following table.

Table 3 TOE Security Assurance Requirements

Assurance Component ID	Assurance Component Name
ADV_FSP.1	Basic functional specification
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.1	Labeling of the TOE
ALC_CMS.1	TOE CM coverage
ATE_IND.1	Independent testing - conformance
AVA_VAN.1	Vulnerability survey

9 Validator Comments/Recommendations

The validation team notes the following:

- Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the device needs to be assessed separately, and no further conclusions can be drawn about their effectiveness. As noted in the Security Target, this includes functional features such as ISSU, OAA, TRILL, MDC, IRF and EVB.
- The TOE supports both IPv4 and IPv6 networks; however, IPv6 was not exercised during any of the assurance activities.
- The validation team notes that the evaluated configuration is dependent upon the TOE being configured for FIPS operation.
- Note that audit records are not buffered for transmission to the syslog server, therefore the administrator is advised to ensure additional audit destinations are configured so that audit logs are not lost in the event of loss of connectivity to a single syslog server.

10 Annexes

Not applicable

11 Security Target

- Hewlett Packard Enterprise MSR Routers 1k-4k Security Target, Version 1.0, February 16, 2016

12 Abbreviations and Acronyms

Abbreviation	Description
AES	Advanced Encryption Standard
CC	Common Criteria
CLI	Command Line Interface
IP	Internet Protocol
IPS	Intrusion Prevention System
NIC	Network Interface Card
PP	Protection Profile
RFC	Request for Comment
SFR	Security Functional Requirement
SFP	Security Function Policy
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Target
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function(s)

13 Bibliography

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

[1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction, Version 3.1, Revision 4, September 2012.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1 Revision 4, September 2012.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012.

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 4, September 2012.

[5] Hewlett Packard Enterprise MSR Routers 1k-4k Security Target, Version 1.0, February 16, 2016

[6] Common Criteria Evaluation and Validation Scheme - Guidance to CCEVS Approved Common Criteria Testing Laboratories, Version 2.0, 8 Sep 2008.

[7] Evaluation Technical Report For Hewlett Packard Enterprise MSR Routers 1k-4k Part 2 (Leidos Proprietary), Version 1.0, February 16, 2016.

[8] Assurance Activities Report for Hewlett-Packard Company MSR 1000, 2000, 3000, and 4000 Series Routers with Comware 7.1 Version 1.0, 16 February 2016.