MOSTI
KEMENTERIAN SAINS, TEKNOLOGI DAN INOVASI
MINISTRY OF SCIENCE, TECHNOLOGY AND INNOVATION

CyberSecurity MALAYSIA
An agency under MOSTI

C070 Certification Report

Hewlett Packard Enterprise HSR6600 Series, HSR6800 Series and MSR1000 Series Routers with Comware V7.1

File name: ISCB-5-RPT-C070-CR-v1
Version: v1
Date of document: 22 April 2016
Document classification: PUBLIC

Malaysian Common Criteria Evaluation & Certification Scheme
MyCC

For general inquiry about us or our services,
please email: mycc@cybersecurity.my

C070 Certification Report

Hewlett Packard Enterprise HSR6600 Series, HSR6800 Series and MSR1000 Series Routers with Comware V7.1

22 April 2016
ISCB Department

CyberSecurity Malaysia

Level 5, Sapura@Mines,
No 7 Jalan Tasik,The Mines Resort City
43300 Seri Kembangan, Selangor, Malaysia
Tel: +603 8992 6888 Fax: +603 8992 6841
http://www.cybersecurity.my

Document Authorisation

DOCUMENT TITLE:	C070 Certification Report
DOCUMENT REFERENCE:	ISCB-5-RPT-C070-CR-v1
ISSUE:	v1
DATE:	22 April 2016

DISTRIBUTION:	UNCONTROLLED COPY - FOR UNLIMITED USE AND DISTRIBUTION

Copyright Statement

Registered office:
Level 5, Sapura@Mines
No 7, Jalan Tasik,
The Mines Resort City,
43300 Seri Kembangan
Selangor Malaysia

Registered in Malaysia – Company Limited by Guarantee
Company No. 726630-U

Printed in Malaysia

Foreword

The Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme has been established under the 9th Malaysian Plan to increase Malaysia's competitiveness in quality assurance of information security based on the Common Criteria (CC) standard and to build consumers' confidence towards Malaysian information security products.

The MyCC Scheme is operated by CyberSecurity Malaysia and provides a model for licensed Malaysian Security Evaluation Facilities (MySEFs) to conduct security evaluations of ICT products, systems and protection profiles against internationally recognised standards. The results of these evaluations are certified by the Malaysian Common Criteria Certification Body (MyCB) Unit, a unit established within Information Security Certification Body (ISCB) Department, CyberSecurity Malaysia.

By awarding a Common Criteria certificate, the MyCB asserts that the product complies with the security requirements specified in the associated Security Target. A Security Target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the Security Target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 22 April 2016 and the Security Target (Ref [6]). The certification report, Certificate of product evaluation and security target are posted on the MyCC Scheme Certified Product Register (MyCPR) at www.cybersecurity.my/mycc and the Common Criteria Portal (the official website of the Common Criteria Recognition Arrangement).

Reproduction of this report is authorized provided the report is reproduced in its entirety.

Disclaimer

The Information Technology (IT) product identified in this certification report and its associated certificate has been evaluated at an accredited and licensed evaluation facility established under the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]) using the Common Methodology for IT Security Evaluation, version 3.1 revision 4 (Ref [3]), for conformance to the Common Criteria for IT Security Evaluation, version 3.1 revision 4 (Ref [2]). This certification report and its associated certificate apply only to the specific version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the MyCC Scheme and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certification report and its associated certificate is not an endorsement of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certification report and its associated certificate, and no warranty of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Document Change Log

RELEASE	DATE	PAGES AFFECTED	REMARKS/CHANGE REFERENCE
d1	7 April 2016	All	Initial draft of certification report
V1	22 April 2016	All	Final version of certification report

Executive Summary

Hewlett Packard Enterprise HSR6600 Series, HSR6800 Series, and MSR1000 Series routers, all with Comware V7.1 are the Target of Evaluation (TOE) for the Evaluation Assurance Level 3 Augmented with ALC_FLR.2.

The HSR6600 Series in the evaluated configuration consists of the following specific devices:

- HP HSR6602-G Router
- HP HSR6602-XG Router

The HSR6800 Series in the evaluated configuration consists of the following specific devices:

- HP HSR6802E Router Chassis
- HP HSR6804E Router Chassis
- HP HSR6808E Router Chassis

Each of these devices requires an HP HSR6800 RSE-X3 Router Main Processing Unit.

The MSR1000 Series in the evaluated configuration consists of the following specific device:

- HP MSR1003-8S AC Router

The various routers comprising the TOE are all Gigabit Ethernet router appliances that consist of hardware and software components. While the physical form factor of each of the three series is substantially different, the underlying hardware shares a similar architecture. The software uses a common code base of a modular nature with only the modules applicable for the specific hardware installed.

The common software code shared on these devices is called Comware. Comware version 7.1 is used in the evaluated configuration. Comware is a special purpose appliance system software that implements a wide array of networking technology, including IPv4/IPv6 dual-stacks, a data link layer, layer 2 and 3 routing, Ethernet switching, Virtual Local Area Networks (VLANs) and Quality of Service (QoS).

The scope of evaluation covers major security features as follows:

a) **Security Audit**: The TOE is able to generate audit records of security-relevant events occurring on the TOE. Generated audit records include a date and time stamp, the nature or type of the triggering event, an indication of the event outcome, and identification of the agent responsible for the event. The TOE provides administrators with the ability to review audit records stored in the audit trail. The audit records are stored on the TOE appliance, where they are protected from unauthorized modification and deletion. The TOE can also be configured to export audit records to an external audit server.

b) **Cryptographic Support**: The TOE implements cryptographic algorithms that provide key management, random bit generation, data encryption and decryption, digital signature generation and verification, 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, which ensures the TOE's configuration is consistent with the FIPS 140-2 standard.

c) **User Data Protection**: The TOE provides firewall capabilities that allow for the definition of firewall rules, collectively known as access control lists (ACLs), which are applied to applicable network traffic as it is received and which would pass through the TOE between connected networks. The ACLs can be basic, with matching criteria based only

on source IP address, or advanced, with matching criteria based on source and destination addresses, transport layer protocol, and service. ACLs can also be defined independently for both IPv4 and IPv6 network traffic and can be assigned to specific TOE interfaces.

d) **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 a locally connected console and a network-accessible interface (via SSHv2) for interactive administrator sessions. The TOE supports the local (that is, 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, for example, centralized user administration.

e) **Security Management**: The TOE provides a command line interface (CLI) to access its 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.

f) **Protection of the TSF**: The TOE implements a number of self-tests that it performs when it starts up, to ensure its cryptographic functions operate properly and that the Comware and TSF executable files have not been modified. The TOE includes its own time source for providing reliable time stamps that are used in audit records

g) **TOE Access**: The TOE will terminate interactive sessions after a period of inactivity configurable by an administrator. The TOE allows administrators to terminate their own interactive sessions.

h) **Trusted path/channels**: The TOE protects interactive communication with administrators using SSHv2 for CLI access. Using SSHv2, both integrity and disclosure protection is ensured. The TOE can be configured to use IPsec to protect communications with external IT entities, such as audit and authentication servers, against disclosure or undetected modification of data.

The scope of the evaluation is defined by the Security Target (Ref [6]) which identifies assumptions made during the evaluation, the intended environment for the TOE, the security function requirements, and the evaluation assurance level at which the product is intended to satisfy the security requirements. Prospective consumers are advised to verify that their operating environment is consistent with the evaluated configuration, and to give due consideration to the comments, observations and recommendations in this certification report.

This report confirms the findings of the security evaluation of the TOE to the Common Criteria (CC) Evaluation Assurance Level 3 (EAL3) Augmented with ALC_FLR.2 This report confirms that the evaluation was conducted in accordance with the relevant criteria and the requirements of the Malaysia Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]).

The evaluation was performed by BAE Systems Applied Intelligence MySEF (Malaysia Security Evaluation Facility) and completed on 6 April 2016.

The Malaysia Common Criteria Certification Body (MyCB), as the MyCC Scheme Certification Body, declares that the TOE evaluation meets all the Arrangements on the Recognition of Common Criteria certificates and the product will be listed in the MyCC Scheme Certified Products Register (MyCPR) at http://www.cybersecurity.my/mycc and the Common Criteria portal (the official website of the Common Criteria Recognition Arrangement) at www.commoncriteriaportal.org.

It is the responsibility of the user to ensure that Hewlett Packard Enterprise HSR6600 Series, HSR6800 Series, and MSR1000 Series routers, all with Comware V7.1 meet their requirements. It is recommended that a potential user of Hewlett Packard Enterprise HSR6600 Series, HSR6800 Series, and MSR1000 Series routers, all with Comware V7.1 refer to the Security Target (Ref [6]) and this Certification Report prior to deciding whether to purchase the product.

Table of Contents

Document Authorisation ii

Copyright Statement iii

Foreword iv

Disclaimer v

Document Change Log vi

Executive Summary vii

Table of Contents x

Index of Tables xi

Index of Figures xi

1 Target of Evaluation 1

1.1 TOE Description 1

1.2 TOE Identification 3

1.3 Security Policy 4

1.4 TOE Architecture 4

1.4.1 Logical Boundaries 5

1.5 Clarification of Scope 7

1.6 Assumptions 7

1.6.1 Usage assumptions 7

1.6.2 Environment assumptions 8

1.7 Evaluated Configuration 8

1.8 Delivery Procedures 8

1.9 Documentation 9

2 Evaluation 10

2.1 Evaluation Analysis Activities 10

2.1.1 Life-cycle support 10

2.1.2 Development 12

2.1.3 Guidance documents 14

2.1.4 IT Product Testing 15
3 Result of the Evaluation 17
3.1 Assurance Level Information 17
3.2 Recommendation 17
Annex A References 18
A.1 References 18
A.2 Terminology 18
A.2.1 Acronyms 18
A.2.2 Glossary of Terms 19

Index of Tables

Table 1: TOE identification 3
Table 2: List of Acronyms 18
Table 3: Glossary of Terms 19

Index of Figures

Figure 1 Comware V7.1 Planes 5

1 Target of Evaluation

1.1 TOE Description

1 The TOE is the Hewlett Packard Enterprise HSR6600 Series, HSR 6800 Series and MSR1000 Series routers, all with Comware V7.1. The HSR6600 Series in the evaluated configuration consists of the following specific devices:

- HP HSR6602-G Router
- HP HSR6602-XG Router

2 The HSR6800 Series in the evaluated configuration consists of the following specific devices:

- HP HSR6802E Router Chassis
- HP HSR6804E Router Chassis
- HP HSR6808E Router Chassis.

3 Each of these devices requires an HP HSR6800 RSE-X3 Router Main Processing Unit.

4 The MSR1000 Series in the evaluated configuration consists of the following specific device:

- HP MSR1003-8S AC Router.

5 The various routers comprising the TOE are all Gigabit Ethernet router appliances that consist of hardware and software components. While the physical form factor of each of the three series of routers is substantially different, the underlying hardware shares a similar architecture. The software uses a common code base of a modular nature with only the modules applicable for the specific hardware installed.

6 The common software code shared on these devices is called Comware. Comware version 7.1 is used in the evaluated configuration. Comware is a special purpose appliance system software that implements a wide array of networking technology, including IPv4/IPv6 dual-stacks, a data link layer, layer 2 and 3 routing, Ethernet switching, Virtual Local Area Networks (VLANs) and Quality of Service (QoS).

7 The HP HSR6600 Series are high-performance services, WAN routers, designed for small-to medium campus WAN edge and aggregation, and high end branch, deployments. These routers are built with a compact multi-core centralized processing architecture that delivers, in a 2 RU form factor, routing, security, full layer 2 switching, and modular WAN and LAN interface options, all integrated in a single routing platform.

8 The HSR6602-G router has 4 dual-personality 1000 Mbps ports and 1 payload slot that can accommodate up to 4 modular interface cards.

9 The HSR6602-XG router, in addition to its 4 dual-personality 1000 Mbps ports and single payload slot, has 2 SPF+ 10GbE ports.

10 The HP HSR6800 Series are high-performance, multiservice router chassis designed for data center interconnection, enterprise WAN core, campus WAN edge, and high-speed WAN aggregation services. These devices feature hardware architecture with multi-core CPUs and fully distributed routing and service engines for increased performance. All engines have separate control and service planes to avoid interference and to facilitate service continuity during an active/standby switchover. The distributed design allows packet forwarding and

complicated services such as NAT, GRE, NetStream, QoS, and IPsec to be processed on each line card independently, thus enhancing the service processing performance of the overall system as line cards are added.

11 The switching fabric connects to the line cards through high-speed passive backplane channels and uses patent distributed scheduling algorithms and virtual output queues (VOQ) to perform inter-card forwarding, implementing non-blocking forwarding and end-to-end traffic control.

12 The devices in this series deliver routing, multicast, MPLS, IPv6, security, quality of service, carrier-level high-availability features, and high-density 10GbE and 1GbE interface options. They support all IPv4 and IPv6 routing protocols including RIP/RIPng, OSPF/OSPFv3, IS-IS/IS-ISv6, BGP/BGP4+, PIM/PIM6, MSDP, MBGP and policy-based routing, delivering increased flexibility. In addition, the series supports comprehensive MPLS features, including LDP, MPLS TE, L3 VPN, L2 VPN, VPLS, Multicast VPN, 6PE, and 6vPE, providing further flexibility.

13 The HP HSR6802E Router Chassis is a 5RU high-performance distributed architecture router platform that supports 2 MPUs in 1+1 redundancy and up to 2 service line cards. It provides up to 1.024 Tbps backplane bandwidth and 120 Mpps throughput via 2 SAP slots or 4 HIM slots or 8 MIM slots, or a combination thereof.

14 The HP HSR6804E Router Chassis is a 7RU high-performance distributed architecture router platform that supports 2 MPUs in 1+1 redundancy and up to 4 service line cards. It provides up to 1.024 Tbps backplane bandwidth and 240 Mpps throughput via 4 SAP slots or 8 HIM slots or 16 MIM slots, or a combination thereof.

15 The HP HSR6808E Router Chassis is a 20RU high-performance distributed architecture router platform that supports 2 MPUs in 1+1 redundancy and up to 8 service line cards. It provides up to 2.048 Tbps backplane bandwidth and 420 Mpps throughput via 8 SAP slots or 16 HIM slots or 32 MIM slots, or a combination thereof.

16 Each of the HSR6800 Series devices requires an HP HSR6800 RSE-X3 Router Main Processing Unit (MPU). The MPU supports the administrative interface for managing the chassis itself as well as the other networking modules installed in the chassis. The MPU provides the following external interfaces:

- Management Ethernet port—a 10Base-T/100Base-TX/1000Base-T autosensing RJ-45 port that allows an administrator to manage the router through a network management server without using any service interface of the router. The management Ethernet port is used only for managing the router and has no service processing capabilities such as data forwarding.
- Console port—RS-232 asynchronous serial port that can be connected to a computer for system debugging, configuration, maintenance, management, and host software loading. It provides local access to the CLI.
- AUX port—RS-232 asynchronous serial port intended as a backup port if the local console port fails

17 The HP MSR1000 Series are high-performance, entry-level, small branch routers that deliver integrated routing, switching, security, mobility, and SIP in a single box. With an integrated infrastructure and modular design, the MSR1000 Series reduces complexity and simplifies the network through integrated routing/ switching/ security/ voice/ 3G and 4G LTE WAN.

18 The MSR1003-8S AC router provides 3 SIC or 1 SIC and 1 DSIC module slots, 2 RJ-45 autosensing 10/100/1000 WAN ports, and 8 RJ-45 autosensing 10/100/1000 LAN ports, supporting up to 500Kpps forwarding and 170Mbps of IPsec encryption throughput.

19 There are security functionalities covered under the scope of the evaluation which are :

- **Security audit**: The TOE is able to generate audit records of security-relevant events occurring on the TOE. Generated audit records include a date and time stamp, the nature or type of the triggering event, an indication of the event outcome, and identification of the agent responsible for the event.
- **Cryptographic support**: The TOE implements cryptographic algorithms that provide key management, random bit generation, data encryption and decryption, digital signature generation and verification, and secure hashing and key-hashing features in support of higher level cryptographic protocols, including IPsec and SSHv2.
- **User data protection**: The TOE provides firewall capabilities that allow for the definition of firewall rules, collectively known as access control lists (ACLs), which are applied to applicable network traffic as it is received and which would pass through the TOE between connected networks.
- **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.
- **Security management**: The TOE provides a command line interface (CLI) to access its 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.
- **Protection of the TSF**: The TOE implements a number of self-tests that it performs when it starts up, to ensure its cryptographic functions operate properly and that the Comware and TSF executable files have not been modified
- **TOE access**: The TOE will terminate interactive sessions after a period of inactivity configurable by an administrator.
- **Trusted path/channels**: The TOE protects interactive communication with administrators using SSHv2 for CLI access.

1.2 TOE Identification

20 The details of the TOE are identified in Table 1 below.

Table 1: TOE identification

Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Project Identifier	C070
TOE Name	Hewlett Packard Enterprise HSR6600 Series, HSR6800 Series, and MSR1000 Series Routers, all with Comware V7.1
TOE Version	Comware V7.1

Security Target Title	Hewlett Packard Enterprise HSR6600 Series, HSR6800 Series, and MSR1000 Series Routers Security Target
Security Target Version	1.0
Security Target Date	10 March 2016
Assurance Level	Evaluation Assurance Level 3 Augmented with ALC_FLR.2
Criteria	Common Criteria for Information Technology Security Evaluation, September 2012, Version 3.1, Revision 4 (Ref [2])
Methodology	Common Criteria for Information Technology Security Evaluation, September 2012, Version 3.1, Revision 4 (Ref [3])
Protection Profile Conformance	None
Common Criteria Conformance	CC Part 2 Conformant CC Part 3 Conformant Package conformant to EAL 3 Augmented (ALC_FLR.2)
Sponsor	Leidos Inc
Developer	Hewlett Packard Enterprise
Evaluation Facility	BAE System Applied Intelligence MySEF

1.3 Security Policy

21 There are no organisational security policies that have been defined regarding the use of the TOE.

1.4 TOE Architecture

22 The TOE includes both logical and physical boundaries as described in Section 2.2 of the Security Target (Ref [6]).

23 Comware is special purpose appliance system software that implements a wide array of networking technology, including: IPv4/IPv6 dual-stacks; a data link layer; layer 2 and 3 routing; Ethernet switching; Virtual Local Area Networks (VLANs); and Quality of Service (QoS). The evaluated version of Comware is V7.1. It should be noted that Comware runs on a variety of underlying architectures including VxWorks, Linux, pSOS and Windows, but the only underlying architecture found in the evaluated configuration is Linux.

24 Comware V7.1 comprises the following four planes, as depicted in **Error! Reference source not found.** below:

- 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—provides data forwarding for local packets and received IPv4 and IPv6 packets at different layers.
- Control plane—comprises all routing, signalling, and control protocols, such as MPLS, OSPF, and security control protocols. It generates forwarding tables for the data plane.
- Management plane—provides a management interface for operators to configure, monitor, and manage Comware V7.1. The management interface comprises a command line interface (CLI) accessed using Secure Shell (SSH).

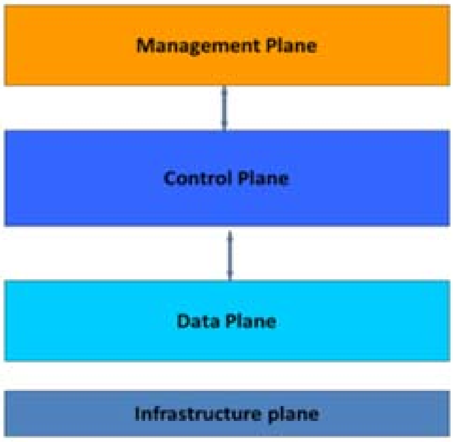

Figure 1 Comware V7.1 Planes

1.4.1 Logical Boundaries

25 The scope of the evaluation was limited to those claims made in the Security Target (Ref [6]) and includes only the following evaluated security functionality:

- Security audit
- Cryptographic support
- User data protection
- Identification and authentication
- Security management
- Protection of the TSF
- TOE access
- Trusted path/channels

26 **Security audit**: The TOE is able to generate audit records of security-relevant events occurring on the TOE. Generated audit records include a date and time stamp, the nature or type of the triggering event, an indication of the event outcome, and identification of the agent responsible for the event. The TOE provides administrators with the ability to review audit

records stored in the audit trail. The audit records are stored on the TOE appliance, where they are protected from unauthorized modification and deletion. The TOE can also be configured to export audit records to an external audit server.

27 **Cryptographic support**: The TOE implements cryptographic algorithms that provide key management, random bit generation, data encryption and decryption, digital signature generation and verification, 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, which ensures the TOE's configuration is consistent with the FIPS 140-2 standard.

28 **User data protection**: The TOE provides firewall capabilities that allow for the definition of firewall rules, collectively known as access control lists (ACLs), which are applied to applicable network traffic as it is received and which would pass through the TOE between connected networks. The ACLs can be basic, with matching criteria based only on source IP address, or advanced, with matching criteria based on source and destination addresses, transport layer protocol, and service. ACLs can also be defined independently for both IPv4 and IPv6 network traffic and can be assigned to specific TOE interfaces.

29 **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 a locally connected console and a network-accessible interface (via SSHv2) for interactive administrator sessions.

The TOE supports the local (that is, 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, for example, centralized user administration.

30 **Security management**: The TOE provides a command line interface (CLI) to access its 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.

31 **Protection of the TSF**: The TOE implements a number of self-tests that it performs when it starts up, to ensure its cryptographic functions operate properly and that the Comware and TSF executable files have not been modified.

The TOE includes its own time source for providing reliable time stamps that are used in audit records.

32 **TOE access:** The TOE will terminate interactive sessions after a period of inactivity configurable by an administrator.

The TOE allows administrators to terminate their own interactive sessions.

33 **Trusted path/channels**: The TOE protects interactive communication with administrators using SSHv2 for CLI access. Using SSHv2, both integrity and disclosure protection is ensured.

The TOE can be configured to use IPsec to protect communications with external IT entities, such as audit and authentication servers, against disclosure or undetected modification of data.

1.4.2 Physical Boundaries

34 A device in the HSR6600 Router Series or MSR1000 Router Series is a physical network appliance with a fixed number of ports, while a device in the HSR6800 Router Series is a

physical network appliance chassis supporting a fixed number of service line cards. Each series also supports a variety of modules that provide a wide range of network ports varying in number, form factor (copper or fiber), and performance (1 – 10 Gb). The TOE can make use of the following external IT entities in its operational environment:

- Syslog server—the TOE can be configured to export generated audit records to an external syslog server.
- RADIUS and TACACS+ servers—the TOE can be configured to use external authentication servers.
- NTP server—the TOE can be configured to use the Network Time Protocol to keep the local hardware-based real-time clock synchronized with other network devices.
- Management workstation—the TOE supports remote administrative access to its command line interface (CLI) via Secure Shell (SSH), the use of which requires SSHv2 client software

1.5 Clarification of Scope

35 The TOE id designed to be suitable for use in well-protected environments that have effective countermeasures, particularly in the areas of physical access, trained personnel and secure communication in accordance with user guidance that is supplied with the product.

36 Section 1.4 of this document described the scope of the evaluation, which is limited to those claims made in the Security Target (Ref [6]). The TOE comprises the Hewlett Packard Enterprise HSR6600 Series, HSR6800 Series, and MSR1000 Series routers, all with Comware V7.1. Each router is a stand-alone network appliance that provides layer 2 switching and layer 3 routing and service functions. Each series of routers comprising the TOE consists of a set of distinct devices (as identified in Section 1.1 of the Security Target (Ref [6]) that differs primarily according to power delivery, performance, and port density. The various routers comprising the TOE are all Gigabit Ethernet router appliances that consist of hardware and software components. While the physical form factor of each of the three series of routers is substantially different, the underlying hardware shares a similar architecture. The software uses a common code base of a modular nature with only the modules applicable for the specific hardware installed. The TOE also supports SNMPv3, but use of this protocol to connect to the TOE is excluded from the evaluated configuration.

37 Potential consumers of the TOE are advised that some functions and services of the overall product have not been evaluated as part of this evaluation. Potential consumers of the TOE should carefully consider their requirement for using functions and services outside of the evaluated configuration.

1.6 Assumptions

38 This section summarises the security aspects of the environment/configuration in which the IT product is intended to operate. Consumers should understand their own IT environments and that required for secure operation of the TOE as defined in the Security Target (Ref [6]).

1.6.1 Usage assumptions

39 Assumptions for the TOE usage as listed in the Security Target:

a) There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

b) The authorized administrators are not careless, wilfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

1.6.2 Environment assumptions

40 In order to provide a baseline for the IT product during the evaluation effort, certain assumptions about the environment the product is to be used in have to be made. This section documents any environmental assumptions made about the IT product during the evaluation. Assumptions for the TOE environment listed in Security Target are:

a) The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

1.7 Evaluated Configuration

41 The Hewlett-Packard Enterprise HSR6600, HSR6800 and MSR1000 Series Routers running Comware V7.1 is a stand-alone network appliance that consists of a chassis, embedded Comware V7.1 operating system and pluggable components providing network connectivity. Comware is special purpose appliance system software that implements a wide array of networking technology, including: IPv4/IPv6 dual-stacks; a data link layer; layer 2 and 3 routing; Ethernet switching; Virtual Local Area Networks (VLANs); and Quality of Service (QoS). Comware runs on a variety of underlying architectures including VxWorks, Linux, pSOS and Windows, but the only underlying architecture found in the evaluated configuration is Linux. The details are described in Section 2.2 of the Security Target (Ref [6]).

1.8 Delivery Procedures

1) Product Orders

Information about these products can be found on the Hewlett Packard Enterprise website (https://www.hpe.com/us/en/home.html). The H3C supply chain ships all hardware products only to the HPE supply chain and the HPE supply chain ships hardware products to the customer. Because the two supply chains are tightly integrated, the two supply chains will be called HPE supply chain in the remainder of the document. When Hewlett Packard Enterprise receives an order for a product, they notify the HPE supply chain department.

1.1 Order Tracking

Each product shipped by the HPE supply chain department is uniquely identified by its order number

1.2 Order Shipment

The HPE supply chain department packages the Hewlett Packard Enterprise products in boxes for shipment. Shipments include the requested hardware and embedded software, while update software/software patches, and configuration guide documents are downloaded from the Hewlett Packard Enterprise website (https://www.hpe.com/us/en/home.html). DHL Express provides a tracking number of each shipment that can be used to track the product from its source to its destination.

1.3 Order Security

The HPE Supply chain department is a commercial organization providing assembly and packaging services for Hewlett Packard Enterprise. DHL express is also a commercial organization providing delivery services. Both supply chain department and DHL are trusted by Hewlett Packard Enterprise to assemble, package, and deliver the products according to Hewlett Packard Enterprise's specifications and without allowing the integrity of the products to be compromised. Additionally, since the packages have labels affixed to them, it would be evident to customers if tampering occurred if the labels were replaced; thus, the security of the product is ensured.

42 All delivery process details are described in Section 4 of the Life Cycle documentation.

1.9 Documentation

43 It is important that the TOE is used in accordance with guidance documentation in order to ensure secure usage of the product.

44 The following documentation is provided by the developer to the end user as guidance to ensure secure delivery, installation and operation of the product:

a) Hewlett Packard Enterprise HSR6600 Series, HSR6800 Series and MSR1000 Series Routers Security Target version 1.0, 10 March 2016

b) Preparative Procedures for CC EAL3 Evaluated Hewlett Packard Enterprise HSR6800, HSR6600 and MSR1000 router series based on Comware V7.1 Revision Version 1.01, 4 January 2016

c) Comware V7 Command Reference for CC Supplement Revision 1.05, 2 December 2015

d) Comware V7 Platform System Log Messages Revision 1.00, 2 December 2015

e) Comware V7 Configuration Guide for CC Supplement Revision 1.6, 2 December 2015

2 Evaluation

45 The evaluation was conducted in accordance with the requirements of the Common Criteria, version 3.1 Revision 4 (Ref [2]) and the Common Methodology for IT Security Evaluation (CEM), version 3.1 Revision 4 (Ref [3]).The evaluation was conducted at Evaluation Assurance Level 3 Augmented with ALC_FLR.2. The evaluation was performed conformant to the MyCC Scheme Policy (MyCC_P1) (Ref [4]) and MyCC Scheme Evaluation Facility Manual (MyCC_P3) (Ref [4]).

2.1 Evaluation Analysis Activities

46 The evaluation activities involved a structured evaluation of the TOE, including the following components:

2.1.1 Life-cycle support

2.1.1.1 Flaw Remediation

47 The evaluators examined the flaw remediation procedures documentation and determined that it described the procedures used to track all reported security flaws in each release of the TOE.

48 The evaluators examined the flaw remediation procedures and determined that the application of these procedures would produce a description of each security flaw in terms of its nature and effects.

49 The evaluators examined the flaw remediation procedures and determined that the application of these procedures would identify the status of finding a correction to each security flaw.

50 The evaluators checked the flaw remediation procedures and determined that the application of these procedures would identify the corrective action for each security flaw.

51 The evaluators examined the flaw remediation procedures documentation and determined that it described a means of providing the TOE users with the necessary information on each security flaw.

52 The evaluators examined the flaw remediation procedures and determined that the application of these procedures would result in a means for the developer to receive from TOE user reports of suspected security flaws or requests for corrections to such flaws.

53 The evaluators examined the flaw remediation procedures and determined that the application of these procedures would result in a timely means of providing registered TOE users (who might be affected) with reports about, and associated corrections to, each security flaw.

54 The evaluators examined the flaw remediation procedures and determined that the application of these procedures would result in automatic distribution of the reports and associated corrections to the registered TOE users who might be affected.

55 The evaluators examined the flaw remediation procedures and determined that the application of these procedures would help to ensure that every reported flaw is corrected.

56 The evaluators examined the flaw remediation procedures and determined that the application of these procedures would help to ensure that the TOE users were issued remediation procedures for each security flaw.

57 The evaluators examined the flaw remediation procedures and determined that the application of these procedures would result in safeguards that the potential correction would contain no adverse effects.

58 The evaluators examined the flaw remediation guidance and determined that the application of these procedures would result in a means for the TOE user to provide reports of suspected security flaws or requests for corrections to such flaws.

59 The evaluators examined the flaw remediation guidance and determined that it describes a means of enabling the TOE users to register with the developer.

60 The evaluators examined the flaw remediation guidance and determined that it identifies specific points of contact for user reports and enquiries about security issues involving the TOE.

2.1.1.2 Configuration Management Capability

61 The evaluators confirmed that the TOE provided for evaluation is labelled with its reference.

62 The evaluators confirmed that the TOE references used are consistent.

63 The evaluators examined the method of identifying configuration items and determined that it describes how configuration items are uniquely identified.

64 The evaluators examined the configuration items in the configuration item list and determined that they are identified in a way that is consistent with the CM documentation. The application of the CM systems was examined during the site visit at H3C Technologies in Beijing, China and the evaluators confirmed that the CI List was consistent with the provided evidence. The evaluators examined the access control measures described in the CM plan and determined that they are effective in preventing unauthorised access to the configuration items.

65 The evaluators confirmed that the CM documentation provided includes a CM plan.

66 The evaluators examined the CM plan and determined that it describes how the CM system is used for the development of the TOE.

67 The evaluators confirmed that the configuration items identified in the configuration list are being maintained by the CM system.

68 The evaluators checked the CM documentation and confirmed that it includes the CM system records identified by the CM plan.

69 The evaluators confirmed that the CM system is being operated in accordance with the CM plan.

2.1.1.3 Configuration Management Scope

70 The evaluators confirmed that the configuration list includes the following set of items:

- the TOE itself;

- the parts that comprise the TOE;
- the TOE implementation representation; and
- the evaluation evidence required by the SARs in the ST.

71 The evaluators confirmed that the configuration list uniquely identifies each configuration item.

72 The evaluators confirmed that the configuration list indicates the developer of each TSF relevant configuration item.

2.1.1.4 TOE Development Security

73 The evaluators examined the development security documentation and determined that it details all security measures used in the development environment that are necessary to protect the confidentiality and integrity of the TOE design and implementation.

74 The evaluators examined the development confidentiality and integrity policies and confirmed the sufficiency of the security measures employed.

75 The evaluators examined the development security documentation and associated evidence and confirmed that the security measures are being applied during the Development Environment Assessment.

2.1.1.5 TOE Delivery

76 The evaluators examined the delivery documentation and determined that it describes all procedures that are necessary to maintain security when distributing versions of the TOE or parts of it to the consumer.

77 The evaluators determined that the delivery procedures are used. All the details are provided in Section 4 of the Life Cycle documentation.

2.1.1.6 TOE Lifecycle Definition

78 The evaluators examined the documented description of the life-cycle model used and determined that it covers the development and maintenance process.

79 The evaluators examined the life-cycle model and determined that use of the procedures, tools and techniques described by the life-cycle model will make the necessary positive contribution to the development and maintenance of the TOE.

2.1.2 Development

2.1.2.1 Architecture

80 The evaluators examined the security architecture description and determined that the information provided in the evidence is presented at a level of detail commensurate with the descriptions of the SFR-enforcing abstractions contained in the functional specification and TOE design.

81 The security architecture description describes the security domains maintained by the TSF.

82 The initialisation process described in the security architecture description preserves security.

83 The evaluators examined the security architecture description and concluded that it contains sufficient information to demonstrate that the TSF is able to protect itself from tampering by untrusted active entities. The security architecture description presents an analysis that adequately describes how the SFR-enforcing mechanisms cannot be bypassed.

2.1.2.2 Functional Specification

84 The evaluators examined the functional specification and determined that:

- the TSF is fully represented,
- it states the purpose of each TSF Interface (TSFI),
- the method of use for each TSFI is given,
- the completeness of the TSFI representation,
- it is a complete and accurate instantiation of the SFRs.

85 The evaluators also examined the presentation of the TSFI and determined that:

- it completely identifies all parameters associated with every TSFI,
- it completely and accurately describes all SFR-enforcing actions associated with every SFR-enforcing TSFI,
- it completely and accurately describes all error messages resulting from an invocation of each SFR-enforcing TSFI,
- it summarises the SFR-supporting and SFR-non interfering actions associated with each TSFI.

86 The evaluators also confirmed that the developer supplied tracing links the SFRs to the corresponding TSFIs.

2.1.2.3 TOE Design Specification

87 The evaluators examined the TOE design and determined that the structure of the entire TOE is described in terms of subsystems. The evaluators also determined that all subsystems of the TSF are identified. The evaluators determined that interactions between the subsystems of the TSF were described.

88 The evaluators examined the TOE and determined that each SFR-non interfering subsystem of the TSF was described such that the evaluators could determine that the subsystem is SFR-non interfering.

89 The evaluators found the TOE design to be a complete, accurate, and detailed description of the SFR-enforcing behaviour of the SFR-enforcing subsystems.

90 The evaluators examined the TOE design and determined that it provided a complete and accurate high-level description of the SFR-supporting and SFR-non interfering behaviour of

the SFR-enforcing subsystems. The evaluators determined that the TOE design provided a complete and accurate high-level description of the behaviour of the SFR-supporting subsystems.

91 The evaluators determined that the TOE design contained a complete and accurate mapping from the TSFI described in the functional specification to the subsystems of the TSF described in the TOE design.

92 The evaluators determined that all Security Target SFRs were covered by the TOE design, and concluded that the TOE design was an accurate instantiation of all SFRs.

2.1.3 Guidance documents

2.1.3.1 Operating Guidance

93 The evaluators examined the operational user guidance b) and determined that it describes, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings. For each role, the secure use of available TOE interfaces is described. The available security functionality and interfaces are described for each user role – in each case, all security parameters under the control of the user are described with indications of secure values where appropriate.

94 The operational user guidance describes, for each user role, each type of security-relevant event relative to the user functions that need to be performed, including changing the security characteristics of entities under the control of the TSF and operation following failure or operational error.

95 The evaluators examined the operational user guidance (in conjunction with other evaluation evidence c),d),e)) and determined that the guidance identifies all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

96 The evaluators determined that the operational user guidance describes, for each user role, the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

97 The evaluators found that the operational user guidance is clear and reasonable.

2.1.3.2 Preparation Guidance

98 The evaluators examined the provided delivery acceptance documentation (contained in 44b)) and determined that they describe the steps necessary for secure acceptance of the TOE in accordance with the developer's delivery procedures.

99 The evaluators determined that the provided installation procedures describe the steps necessary for secure installation of the TOE and the secure preparation of the operational environment in accordance with the security objectives in the ST.

100 The evaluators performed all user procedures necessary to prepare the TOE during testing and determined that the TOE and its operational environment can be prepared securely using only the supplied preparative user guidance.

2.1.4 IT Product Testing

101 Testing at EAL3 consists of assessing developer tests, performing independent functional tests, and performs penetration tests. The TOE testing was conducted by evaluators for BAE Systems Applied Intelligence MySEF. The detailed testing activities, including configurations, procedures, test cases, expected results and actual results are documented in a separate Test Plan Reports.

2.1.4.1 Assessment of Developer Tests

102 The evaluators verified that the developer has met their testing responsibilities by examining their test plans, and reviewing their test results, as documented in the Evaluation Technical Report (Ref [7]) (not a public document because it contains information proprietary to the developer and/or the evaluator).

103 The evaluators analysed the developer's test coverage and found them to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the interfaces in the functional specification, TOE design and security architecture description was complete.

2.1.4.2 Independent Functional Testing

104 At EAL3, independent functional testing is the evaluation conducted by evaluator based on the information gathered by examining design and guidance documentation, examining developer's test documentation, executing sample of developer's test plan and creating test cases that augmented developer tests.

105 All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The results of the independent functional tests were developed and performed by the evaluators and are consistent with the expected test documentation.

Test ID	Description	Security Function	Justification
F001	• Audit records are protected from unauthorised modifications or deletion. • Ensure that only network-admin and network-operator can view the TOE audit trail file. • Ensure that only security-audit role has exclusive access to seclog.log file.	FAU_GEN.1.1, FAU_GEN.1.2, FAU_GEN.2.1, FAU_SAR.1.1, FAU_SAR.1.2, FIA_UID.2.1.	This test aims to verify that the TOE performs specifications of management functions, user authentication and verification for logged data to ensure only authorized user can perform privilege access to the audit log.
F002	• TOE is able to change next main start-up as FIPS-mode or non-FIPS mode.	FPT_TST.1.1.	This test aims to verify that the TOE is able to be configured as fips-mode or non fips-mode on the next main start-up.
F003	• Demonstrate that the TOE can terminate inactive sessions by an administrator – configured period of time. • Demonstrate that only network-admin role able to	FTA_SSL.3.1, FTA_SSL.4.1, FMT_SMR.1.1, FMT_SMR.1.2.	This test aims to verify that the TOE is able to automatically end a user's inactive session after a network-admin configured time interval and ensure that only Network – Admin role is able to set

Test ID	Description	Security Function	Justification
	set time duration for inactive session.		the inactive session configuration time interval.

106 All testing performed by evaluators produced the expected results and as such the TOE behaved as expected.

2.1.4.3 Penetration Testing

107 The evaluators performed vulnerability analysis of the TOE in order to identify potential vulnerabilities in the TOE. This vulnerability analysis considered public domain sources and an analysis of guidance documentation, functional specification, and TOE design and security architecture description.

108 From the vulnerability analysis, the evaluators conducted penetration testing to determine that the TOE is resistant to attack performed by an attacker possessing a basic attack potential. The following factors have been taken into consideration during penetration tests:

a) Time taken to identify and exploit (elapse time);

b) Specialist technical expertise required (specialised expertise);

c) Knowledge of the TOE design and operation (knowledge of the TOE);

d) Window of opportunity; and

e) IT hardware/software or other requirement for exploitation.

109 The penetration tests focused on:

a) Packet Attribute Analysis

b) Intelligent Fuzzing

c) SSL Heartbleed

d) Denial of Service

110 The results of the penetration testing note that there is no residual vulnerability found. However, it is important to ensure that the TOE is used only in its evaluated configuration and in a secure environment as specified in the Security Target (Ref [6]).

2.1.4.4 Testing Results

111 Tests conducted for the TOE produced the expected results and demonstrated that the product behaved as specified in its Security Target (Ref [6]) and its functional specification. In addition, the documentation supplied as evidence for the EAL3+ ALC_FLR.2 Common Criteria evaluation of the TOE was analyzed to identify possible vulnerabilities.

3 Result of the Evaluation

112 After due consideration during the oversight of the execution of the evaluation by the certifiers and of the Evaluation Technical Report (Ref [7]), the Malaysian Common Criteria Certification Body certifies the evaluation of Hewlett Packard Enterprise HSR6600 Series, HSR6800 Series and MSR1000 Series Routers, all with Comware V7.1 performed by BAE System Applied Intelligence MySEF.

113 BAE System Applied Intelligence MySEF found that Hewlett Packard Enterprise HSR6600 Series, HSR6800 Series and MSR1000 Series Routers, all with Comware V7.1 upholds the claims made in the Security Target (Ref [6]) and supporting documentation, and has met the requirements of the Common Criteria (CC) assurance Level 3 Augmented with ALC_FLR.2 (EAL3+ ALC_FLR.2).

114 Certification is not a guarantee that a TOE is completely free of exploitable vulnerabilities. There will remain a small level of risk that exploitable vulnerabilities remain undiscovered in its claimed security functionality. The risk is reduced as the certified level of assurance increases for the TOE.

3.1 Assurance Level Information

115 EAL 3 provides assurance by a full security target and analysis of the SFRs in that Security Target, using a functional and interface specifications, guidance documentation and a basic description of the architecture of the TOE, to understand the security behaviour.

116 The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, security architecture description and guidance evidence provided) demonstrating resistance to an attacker possessing a Basic attack potential.

117 EAL 3 also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

3.2 Recommendation

118 The following recommendations are made:

a) Potential purchasers of the TOE should review the intended operational environment and ensure that they are comfortable that the stated security objectives for the operational environment can be suitably addressed.

b) The users should make themselves familiar with the developer guidance provided with the TOE and pay attention to all security warnings.

Annex A References

A.1 References

[1] Arrangement on the recognition of Common Criteria Certificates in the field of Information Technology Security, July, 2014.

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

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

[4] MyCC Scheme Policy (MyCC_P1), v1d, CyberSecurity Malaysia, February 2016.

[5] MyCC Scheme Evaluation Facility Manual (MyCC_P3), v1c, February 2016.

[6] Hewlett Packard Enterprise HSR6600 Series, HSR6800 Series and MSR1000 Series Routers Security Target, Version 1.0, 10 March 2016

[7] Evaluation Technical Report, Version 1.0, 6 April 2016

A.2 Terminology

A.2.1 Acronyms

Table 2: List of Acronyms

Acronym	Expanded Term
CB	Certification Body
CC	Common Criteria (ISO/IEC15408)
CEM	Common Evaluation Methodology (ISO/IEC 18045)
CCRA	Common Criteria Recognition Arrangement
IEC	International Electrotechnical Commission
ISO	International Organisation for Standardization
ISCB	Information Security Certification Body
MyCB	Malaysian Common Criteria Certification Body
MyCC	Malaysian Common Criteria Evaluation and Certification Scheme
MyCPR	MyCC Scheme Certified Products Register
MySEF	Malaysian Security Evaluation Facility
PP	Protection Profile
ST	Security Target

Acronym	Expanded Term
TOE	Target of Evaluation

A.2.2 Glossary of Terms

Table 3: Glossary of Terms

Term	Definition and Source
CC International Interpretation	An **interpretation** of the CC or CEM issued by the CCMB that is applicable to all CCRA participants.
Certificate	The official representation from the CB of the certification of a specific version of a product to the Common Criteria.
Certification Body	An organisation responsible for carrying out **certification** and for overseeing the day-today operation of an **Evaluation and Certification Scheme**. Source CCRA
Consumer	The organisation that uses the certified product within their infrastructure.
Developer	The organisation that develops the product submitted for CC evaluation and certification.
Evaluation	The assessment of an IT product, IT system, or any other valid target as defined by the scheme, proposed by an applicant against the standards covered by the scope defined in its application against the certification criteria specified in the rules of the scheme. Source CCRA and MS-ISO/IEC Guide 65
Evaluation and Certification Scheme	The systematic organisation of the functions of **evaluation** and **certification** under the authority of a **certification body** in order to ensure that high standards of competence and impartiality are maintained and that consistency is achieved. Source CCRA.
Interpretation	Expert technical judgement, when required, regarding the meaning or method of application of any technical aspect of the criteria or the methodology. An interpretation may be either a **national interpretation** or a **CC international interpretation**.
Certifier	The certifier responsible for managing a specific certification task.
Evaluator	The evaluator responsible for managing the technical aspects of a specific evaluation task.
Maintenance Certificate	The update of a Common Criteria certificate to reflect a specific version of a product that has been maintained under the MyCC Scheme.

Term	Definition and Source
National Interpretation	An **interpretation** of the CC, CEM or MyCC Scheme rules that is applicable within the MyCC Scheme only.
Security Evaluation Facility	An organisation (or business unit of an organisation) that conducts ICT security evaluation of products and systems using the CC and CEM in accordance with Evaluation and Certification Scheme policy
Sponsor	The organisation that submits a product for evaluation and certification under the MyCC Scheme. The sponsor may also be the developer.

--- END OF DOCUMENT ---