Indian CC Certification Scheme (IC3S)

Certification Report

Report Number:	**STQC/CC/14-15/15/CR**
Product / system:	Router operating system: Comware V7.1 running on MSR2000, MSR3000, and MSR4000 Series Routers

Dated: 27th Dec 2016

Version: 1.0

Government of India
Ministry of Communication & Information Technology
Department of Electronics and Information Technology
Standardization, Testing and Quality Certification Directorate
6. CGO Complex, Lodi Road, New Delhi – 110003
India

This report contains a total of 15 pages. In case it needs to be reproduced, all the pages must be included.

Product developer:	**Hewlett-Packard Company**
TOE evaluation sponsored by:	Hewlett-Packard, 153 Taylor Street, Littleton, MA 01460
Evaluation facility:	ERTL(E)-CCTL, ERTL (East), DN-Block, Sector V, Salt Lake, Kolkata-700091, India.
Evaluation Personnel:	Debasish Jana Malabika Ghose Subhendu Das
Evaluation report:	STQC IT (KOL)/STQC/CC/1415/15/ETRv1.0
Validation Personnel:	Alok Sain

Table of Contents

Contents

PART A: CERTIFICATION STATEMENT AND BACKGROUND OF THE CERTIFICATION BODY

A1 Certification Statement

The product below has been evaluated under the terms of the Indian Common Criteria Certification Scheme (IC3S) and has met the stated Common Criteria requirements. The scope of the evaluation and the assumed usage environment are specified in the body of this report.	
Sponsor	Hewlett-Packard,153 Taylor Street, Littleton, MA 01460
Developer	Hewlett-Packard Company
Product and Version	Comware V7.1.049 running on MSR2000, MSR3000, and MSR4000 Series Routers router hardware"
Security Target	Security Target identification: Hewlett-Packard Company Comware V7.1 Running on MSR2000, MSR3000, and MSR4000 Series Routers Security Target, version 0.11
Brief description of product	The Target of Evaluation (TOE) is 'Comware V7.1.049 running on MSR2000, MSR3000, and MSR4000 Series Routers router hardware'. The TOE is intended to protect the IP packets against incorrect routing caused by unauthorized changes in the network configuration. There are variations in 'hardware configuration' and 'performance' among the different models of the routers, as stated in ST. While the routers have fixed ports, they also support plug-in modules; transceivers, memory, and power supplies that provide additional functionality (e.g., various numbers and types of network connection ports). These plug-in accessories do not serve to change the security characteristics of the TOE and as such can optionally be used in thee valuated configurations. The Comware 7 image files contain the operating system along with the software components required for specific hardware of the series.
CC Part 2 [CC-II]	Conformant
CC Part 3 [CC-III]	Conformant
EAL	EAL3
Evaluation Lab	Common Criteria Test Laboratory, ERTL(E), Kolkata
Date Authorized	Dec 27, 2016

A2. About the Certification Body

STQC IT Certification Services, the IT Certification Body of Standardization Testing and Quality Certification – was established in 1998 and offers a variety of services in the context of security evaluation and validation. It is the first Certification Body in India for BS 7799/ISO 27001 certification of Information Security Management Systems (ISMS). The Indian CC Certification Scheme (IC3S) is the IT security evaluation & certification Scheme based on Common Criteria standards, it is established by Govt. of India under Department of Information Technology, STQC Directorate to evaluate & certify the trustworthiness of security features in Information Technology (IT) products and systems. The IC3S is an Indian independent third party evaluation and certification scheme for evaluating the security functions or mechanisms of the IT products. It also provides

framework for the International Mutual Recognition of such certificates with the member countries of CCRA (Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security). The principal participants in the scheme are-

a) Applicant (Sponsor/Developer) of IT security evaluations;
b) STQC Certification Body (STQC/MeiTY/Govt. of India);
c) Common Criteria Testing Laboratories (CCTLs).

A3 Specifications of the Certification Procedure

The certification body operates under the official administrative procedures according to the criteria and procedures laid down in the following:

- ISO/IEC Guide 65, and the requirements laid down in Annex C of CCRA
- Indian Common Certification Scheme (IC3S)
- STQC/CC/DO2: Standard Operating Procedure (SOP) for Certification Body - Quality Manual – describes the quality management system for the Scheme.
- Common Criteria for Information Technology Security Evaluation (CC) part 1-3, Version 3.1
- Common Evaluation Methodology (CEM) Version 3.1.

A4 Process of Evaluation and Certification

The certification body monitors each individual evaluation to ensure uniform procedures, interpretations of the criteria, and ratings. The TOE has undergone the certification procedure at **STQC IT Certification Body**. The evaluation of the product was conducted by the evaluation body Common Criteria Test Laboratory (CCTL), ERTL (East), DN Block, Sector V, Salt Lake, Kolkata-700091, India. Hereafter this has been referred as CCTL. The evaluation facility is recognized under the IC3S scheme of STQC IT Certification Body.

Hewlett-Packard Company is the developer of the TOE and Hewlett-Packard, 153 Taylor Street, Littleton, MA 01460 is the sponsor.

The certification process is concluded with the completion of this certification report.

This evaluation was completed on 10th Feb 2016 after submission of [ETR] to the certification body. The confirmation of the evaluation assurance level (EAL) only applies on the condition that

- all stated condition regarding configuration and operation, as given in part B of this report, are observed,
- The product is operated – where indicated – in the environment described.

This certification report applies only to the version and release of the product indicated here. The validity of the certificate can be extended to cover new versions and releases of the product, provided the applicant applies for re-certification of the modified product, in accordance with the procedural requirements, and provided the evaluation does not reveal any security deficiencies.

A5 Publication

The following Certification Results consist of Sections B1 to B11 of this report. The TOE will be included in the list of the products certified under IC3S Scheme of STQC IT Certification Body. The list of certified products is published at regular intervals in the Internet at http://www.commoncriteria-india.gov.in. Further copies of this certification report may be ordered from the sponsor of the product. The certification report may also be obtained in electronic form on request to the Certification Body.

PART B: CERTIFICATION RESULTS

B.1 Executive Summary

B.1.1 Introduction

The Certification Report documents the outcome of Common Criteria security evaluation of Router Operating System, "Comware V7.1 running on MSR2000, MSR3000, and MSR4000 Series Routers". It presents the evaluation results and the conformance results. This certificate is intended to assist the prospective buyers and users when judging the suitability of the IT security of the product for specified requirements.

Prospective buyers and users are advised to read this report in conjunction with the referred [ST] of the product, which specifies the functional, environmental and assurance requirements.

The evaluation was performed by Common Criteria Test Laboratory (CCTL), ERTL (East), DN Block, Sector V, Salt Lake, Kolkata-700091, India. The information in the test report is derived from the [ST] written by the developer and the Evaluation Technical Report [ETR] written by Common Criteria Test Laboratory [ERTL (E)-CCTL], ERTL (EAST), Block-DN Sector-V, Kolkata. The evaluation team determined the product to be CC Version 3.1, Part 2 and Part 3 conformant and concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL3) have been met.

B 1.2 Evaluated product and TOE

The product evaluated was:
The Target of Evaluation (TOE) is 'Comware V7.1.049 running on MSR2000, MSR3000, and MSR4000 Series Routers hardware'. The TOE is intended to protect the IP packets against incorrect routing caused by unauthorized changes in the network configuration.
There are variations in 'hardware configuration' and 'performance' among the different models of the routers, as stated in ST. While the routers have fixed ports, they also support plug-in modules; transceivers, memory, and power supplies that provide additional functionality (e.g., various numbers and types of network connection ports). These plug-in accessories do not serve to change the security characteristics of the TOE and as such can optionally be used in the valuated configurations. The 'Comware 7.1' image files contain the operating system along with the software components required for specific hardware of the series.
The evaluated sub-set and configuration of the product is described in this report as the Target of Evaluation (TOE). The Evaluated Configuration, its security functions, assumed environment, architectural information and evaluated configuration are given below (Refer B2 to B5).

B 1.3 Security Claims

The [ST] specifies the security objectives of the TOE and the threats that they counter (Refer 4.1 of ST). All the Security Functional Requirements (SFRs) (listed in 6.1 of ST) are taken from CC Part 2.

B 1.4 Conduct of Evaluation

The evaluation was initiated by the IC3S Certification Scheme of STQC IT Certification Body vide communication no. STQC/CC/1415/15 dated 24th March 2015.
The TOE as described in the [ST] is a dedicated router operating system running on the specified hardware platform.

The TOE was evaluated through evaluation of its documentation, visit of the delivery site; testing and vulnerability assessment using methodology stated in Common Evaluation Methodology [CEM] and ERTL (E)-CCTL, Kolkata Operating Procedure OP-07.
The evaluation has been carried out under written agreement [dated Feb 2016] between ERTL (E)-CCTL, Kolkata and the sponsor.

B 1.5 Independence of Certifier

The certifier did not render any consulting or other services for the company ordering the certification and there was no relationship between them which might have an influence on this assessment.

B 1.6 Disclaimers

The certification results only apply to the version and release of the product as indicated in the certificate. The certificate is valid for stated conditions as detailed in this report. This certificate is not an endorsement of the IT product by the Certification Body or any other organization that recognizes or gives effect to this certificate. It is also not an endorsement of the target of evaluation (TOE) by any agency of the Government of India and no warranty of the TOE is either expressed or implied.

B 1.7 Recommendations and conclusions

The conclusions of the Certification Body are summarized in the Certification Statement at Section A1.
The specific scope of certification should be clearly understood by reading this report along with the [ST].
The TOE should be used in accordance with the environmental assumptions mentioned in the [ST].
The TOE should be used in accordance with the supporting guidance documentation.
This Certification report is only valid for the evaluated configurations of the TOE.

B 2 Identification of TOE

The TOE is identified as:
There are three software packages for these three environments, in the form of **.IPE** files. The software images files are uniquely identified according to the scheme, defined in the Configuration Management system of Hewlett-Packard Company. The integrity of the image files are ensured through validation of its digital signature during installation. The validation of digital signature is a prerequisite for installation of the **.IPE** files on the hardware box/chassis.

B 3 Security policy

There are no organizational security policies that the TOE must meet.

B.4 Assumptions

B.4.1 Personnel assumptions

Assumption code	Description
A.DIRECT	Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the TOE.
A.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
A.REMACC	Authorized administrators may access the TOE remotely from the internal and external networks.

B.4.2 Physical Environmental Assumptions

Physical Assumptions

Assumption code	Description
A.PHYSEC	The TOE is physically secure.

IT Environment Assumptions

Assumption code	Description
A.GENPUR	There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.
A.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE
A.PUBLIC	The TOE does not host public data
A.LOWEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.

B.5 Evaluated configuration

The TOE operates on three types of hardware. These three types hardware environment were supplied by the developer during evaluation. There are three software packages for these three environments, in the form of .IPE files as listed in Table below. The software images files are uniquely identified according to the scheme, defined in HP CM system. The integrity of the image files are ensured through digital signature, validation of which is a prerequisite for installation of the .IPE files on the hardware box/chassis. The **.IPE** files were installed and configured on respective hardware platforms as per the preparatory guidance document of the TOE on the respective models for the purpose of evaluation.

While the routers have fixed ports, they also support plug-in modules; transceivers, memory, and power supplies that provide additional functionality (e.g., various numbers and types of network connection ports). These plug-in accessories do not serve to change the security characteristics of the TOE and as such can optionally be used in thee valuated configurations. The three evaluated instantiations of the TOE are detailed in the table:

The image files	Hardware platform	File size	Hash values (MD5)of the image files
MSR2000-CMW710-R0106P02.IPE	HP MSR2000; MSR2003 AC Router (JG411A)	57.1 MB	2830f7647c530b765fb8dbf7b50932c2
MSR3000-CMW710-R0106P02.IPE	HP MSR3000; MSR3064 Router (JG404A)	58.1 MB	631b9442dc4ff08c75551052f39583d3
MSR4000-CMW710-R0106P02.IPE	HP MSR4000; MSR4060 Router Chassis (JG403A)	80.1 MB	ff6341aa40afd735a1b6936e12afef34

The CAVP certificate numbers of the Crypto module used in the TOE are as follows:

a) **For Comware 7.1** : AES: #2927, TDES: #1740, DSA: #868, ECDSA: #527, SHA: #2463, RNG: #1291, HMAC: #1854, Component Test: #330, RSA: #1543

b) **For MSR HW Accelerators**: AES; #2928, TDES: #1741, DSA: #869, SHA; #2464, HMAC: #1855; RSA: #1541

B.6 Document evaluation

B.6.1 Documentation

The list of documents, those were presented, as evaluation evidences to the evaluators at the evaluation facility, are given below:

1. **Security Target**: Hewlett-Packard Company Comware V7.1 Running on MSR2000, MSR3000, and MSR4000 Series Routers Security Target, version 0.11.

2. **TOE Architecture/Functional Specification and Design description**: Hewlett-Packard Company MSR2000, MSR3000, MSR4000 Series Routers running Comware V7 Design Document Revision 1.3.
3. **Operational User Guidance**: available at www.hp.com
4. **Preparative procedures**: Preparative Procedures for CC EAL2 Evaluated Hewlett-Packard Company MSR2000, MSR3000, and MSR4000 Series Routers Running Comware V7.1, Revision 1.31.
5. **Configuration Management, Capability /scope and TOE delivery**: Hewlett-Packard Company Life Cycle Document, Revision 1.5.
6. **Test cases, logs and coverage**: Test Documentation For MSR2000, MSR3000, MSR4000 Series Routers Running Comware V7.1, V1.03.

B.6.2 Analysis of document

The documents related to the following areas were analyzed using [CEM]. The summary of analysis is as below:

Development process: The evaluators analyzed the functional specification of the TOE and found that the TOE security function interfaces are described clearly and unambiguously. The evaluators also analyzed design and architectural descriptions of the TOE and determined that the only subsystem of the TOE (i.e. router subsystem) is clearly described in the design description. The evaluators determined that architectural description of the TOE includes secure initialization of the TOE and also means of protection of the TOE from tampering and bypassing. The architectural description also shows separation among different planes (Management, Control and Data planes) of 'Comware v7.1'.

Guidance Documents: The evaluators analysed guidance documents like preparative procedure and operational user guidance (presented in the form of website links) and determined that preparative procedure describes clear and unambiguous steps to bring the TOE to its secure state. The operational user guidance information were used from the linked websites during evaluation and found them clear and unambiguous.

Life-cycle support documents: The Life cycle support process document, containing information on Configuration Management and Delivery Procedure were evaluated.

Configuration management: The evaluators analyzed configuration management documentation and determined that the TOE and its associated documents are clearly identified as configurable items. The evaluators also analyzed access control measures defined in the documentation and found satisfactory**.**

Delivery procedure: The delivery procedure document was audited with the objective to ascertain whether it covers secure delivery of the TOE to the end-users. The secure delivery procedure has been described in the document and the same has been audited by the evaluators during their site visit. The end-users can check integrity of the evaluated TOE using hash value of that, if felt necessary.

The final version of the respective evaluation evidences were found to comply with the requirements of CCv3.1 for EAL3.

B.7 Site visit

B.7.1 Objective of Site Visit

The development site of HPE, located at 153 Taylor Street, Littleton, MA, USA was visited by the evaluators in connection with Common Criteria evaluation (EAL3) of the TOE (Target of Evaluation), COMWARE V7.1, to ascertain that the procedures relating to requirements of the class ALC are followed in practice, as described in the documentation.

The site visit objectives are preciously described below against each area of activities/ issues:

Configuration Management System:

- To observe the use of the CM system as described in the CM documentation
- To evidence application of Configuration Management System to ensure that the integrity of the TOE is preserved throughout its life cycle

Delivery Procedure:

- To evidence measures, procedures, and standards concerned with secure delivery of the TOE, ensuring that the security protection offered by the TOE is not compromised during the transfer to the user.
- To observe the practical application of delivery procedures as described in the delivery documentation.

Security measures of the development environment:

- To observe the security measures, implemented by the developer during development and maintenance of the TOE and its consistency with that described in the development security documentation.

B.7.2 Summary of Observations:

Configuration Management System

- The configuration management (CM) system of the organization is documented in the 'HP Life Cycle Document'. The process, as defined in the document, was verified during the site visit.
- The CM systems maintained in development site, China consists of a SVN system, a repository referred as PDM and Lotus Notes. The SVN system is used to maintain the TOE image, constituent source code files and required run-time libraries. The PDM repository is used to maintain documentations relating to the TOE e.g. design documents, life cycle documents, guidance documents and documents relating to testing etc. Lotus note is used to store documents which are intended for sharing with end users through website links, e.g. release notes
- A Unix system is used to store and control the TOE, related Source codes and run time libraries at the development site, Littleton, USA,. The Configuration Items (CI) identification, storage and change control methods were witnessed by the evaluators. The directory structure used to store the source code and libraries, after those are received from China development site, was observed.
- Build (image) generation process including build naming convention was observed. Directory naming convention for storage of different versions of TOE and their constituent source codes and libraries were witnessed.
- Physical access to the lab (located in Room 261 in 1st floor) is controlled through Card based Access control system. The members working in the team (referred as US-BUILD team) are given logical access to the Unix System which is used for storage of the Configuration Items (CI) only when they are physically inside the lab. The Servers are located in a caged area inside the lab and those are logically accessed through terminal located outside the cage area.
- Back up of the system is maintained in a backup server.
- The repositories, PDM System and Lotus note, maintained at development site in China was remotely accessed from Littleton and demonstrated to the evaluators.
- Evidences (screenshots) in support of maintenance of the SVN repository for source files at the development site, China were provided to the evaluators.

Delivery Procedure

- The TOE is delivered to the end user through Hewlett Packard website and the specific link for downloading the TOE is given in the preparative procedure document. A digital signature is used to ensure integrity of the TOE.
- Hardware products necessary to run the TOE is delivered through HP/H3C supply chain department and DHL, a courier service organization. The process adopted, in general, for packaging the products by the HP/H3C department before those are transferred to DHL for delivery to the destination was explained

and demonstrated to the evaluators. Use of labeling information for identification of the packaged product and source and destination on the cartoon boxes were explained. Use of a Quality seal on the 1st layer of packaging for identification of any unauthorized opening of the package which is done by HP/H3C supply chain department was demonstrated. The integrity of the hardware and any embedded software is thus protected during transportation by DHL from source to the destination. The arrangement was found satisfactory.

Security Measures of development environment

Development activities of the TOE are spread in the following two locations:

- H3C, China
- HPE, Littleton, MA, USA

Design and development of the TOE is primarily carried out in H3C, China. The final or last activity of the development process is generation of the build (TOE image) and this activity is carried out at HPE, Littleton, USA.

H3C, China is certified against Information Security Management System standard, ISO/IEC 27001: 2013. The Certificate Number is 179373-2015-AIS-RGC-UKAS dated 20 July, 2015 and the Certificate is valid till 20 July, 2018. A copy of the certificate was presented to the evaluators.

The development site at Littleton, MA, USA was visited to witness the security measures adopted in the same location particularly in respect of physical security and infrastructures, organizational measures, Personnel measures, Access control, policies and practices relating to data protection, Contingency plan etc. The security measures adopted by the organization are found to be satisfactory and adequate to ensure integrity of the TOE.

B 8 Product Testing

Testing at EAL3 consists of the following three steps: Testing by developer, Independent Testing by Evaluation Team, and Penetration testing.

B 8.1 IT Product Testing by Developer

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the [ETR].

The evaluators analyzed the developer's test coverage and found them to be complete and satisfactory. The correspondence between the tests identified in the developer's test documentation and the functional specification and TOE design was complete.

B 7.2 IT Product Independent Testing by Evaluation Team

The evaluators' independent functional testing effort is summarized as below.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and reproducibility of results.

The evaluators have examined the TOE, 'Comware V7.1.049 running on MSR2000, MSR3000, and MSR4000 Series Routers router hardware', and it is found to be configurable as per the description given in the developer's preparative guidance document. It is also observed that the test configuration is consistent with the description as given in the security target document. Highlights of Independent testing are given below:

The TOE, 'Comware V7.1.049 running on MSR2000, MSR3000, and MSR4000 Series Routers router hardware', has been installed properly as per the preparative procedure AGD_PRE document.

The evaluators have repeated the developer's test at CCTL, Kolkata to confirm the reproducibility of the test results.

While making the test strategy for independent testing, consideration is given to cover the security requirements, as well as the security specification as defined in the security target, interfaces

available to the users to cover each of security functional requirements, TOE design and security architecture information. Independent testing is designed to verify the correct implementation of security functionalities available to different levels of users and to check whether audit is being generated for auditable events.

The tests were designed to cover following TSFs and associated TSFIs of the TOE:

a. Security Audit

The TOE is designed to generate log records for a wide range of security relevant and other events as they occur. The events, those can cause an audit record, include starting and stopping the audit function as well as other auditable events as described in "Security Target" document. The audited events of the TOE include: administrative activities, authentication activities and events, access control events, failures of trusted channels etc. The logs can be stored in the TOE as well as to external log server as the TOE is compatible with SYSLOG. The internal audit log operates as a circular buffer that overwrites the oldest records when it becomes full. The TOE can be configured to send generated audit records to an external SYSLOG server in to mitigate the possibility of losing audit records.

b. Cryptographic support

The TOE includes crypto-module providing supporting cryptographic functions. The TOE supports SSHv2 with AES (CBC) 128 or 256 bit keys in conjunction with HMAC-SHA-1 or HMACSHA-1-96 and user authentication using RSA key pairs. It uses a random number generator to generate keys of 128, 192 or 256-bits which support AES CBC encryption. The AES implementation satisfies FIPS PUB 197. The TOE implementation of HMAC-SHA-1 and HMACSHA-1-96 meets FIPS PUB 198-1 and FIPS PUB 180-4. The TOE generates RSA key pairs of 2048 bits in accordance with FIPS PUB 186-3, "Digital Signature Standard (DSS)", Appendix B.3 for RSA schemes.

The TOE supports SNMPv3 using AES (CBC) with 128 bit keys in conjunction with HMAC-SHA-1-96.The TOE implementation of SHA-1 meets FIPS PUB 180-4. The TOE supports IPsec AH and ESP using AES (CBC) with 128, 192 or 256 bit keys and HMAC-SHA-1-96.The TOE does not generate certificates.

Additionally, the TOE is designed to zeroize the cryptographic keys of all types when they are no longer required by the TOE in a manner designed to conform to FIPS 140-2.

c. User data protection

The TOE is designed to ensure its own internal integrity as well as to protect user data from potential, unintended reuse by clearing resources (e.g., memory) as they are allocated to create objects used in the implementation of the

TOE operations. The TOE includes firewall functions that allow the definition of firewall rules, collectively known as access control lists (ACLs), that are applied to applicable network traffic as it is received and 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 management users of the TOE are required to be identified and authenticated before accessing the TOE. In the evaluated configuration, users can connect to the TOE via a local console or remotely using SNMPv3 or SSHv2. In each case, the user is required to log-in, prior to establish a successful session through which TOE functions can be exercised.

The user must provide an identity and also authentication data (e.g., password or password with RSA credentials used in conjunction with an SSH session) that matches the provided identity to establish a session either through console or network.

The TOE uses local authentication by default, however, a Network Administrator can specifically identify an external authentication mechanisms (local, RADIUS, and/or TACACS+) and the order in which they will be used. External authentication mechanisms are not part of the TOE. In case of non-availability of external authentication service (e.g., RADIUS server cannot be reached), the TOE will use the next configured authentication mechanism.

e. Security management

The TOE provides Command Line interface commands to access the wide range of security management functions. The TOE implements a role mechanism that is used to specify the role(s) and corresponding permissions which authenticated users possess. Security management commands are limited to administrators only, which can be executed after successful identification and authentication.

The TOE provides the command line interface for user account management (used for authentication and authorization), system time setting, and system shutdown and re-start. By providing the access control function for the system management services, the TOE ensures that the functions are accessible only to users, authorized with the appropriate management privileges; thus realizing secure management.

f. Protection of the TSF

The hardware of the TOE is a router that includes a hardware-based real-time clock. The embedded Operating System of the TOE manages the clock and exposes clock-related functions for use by the TOE. The TOE software can also be configured to utilize the NTP protocol to keep the local hardware-based real-time clock synchronized with other network devices.

During start-up of the TOE, the TOE first checks the integrity of the Comware and TSF executable files, and then runs a series of self-tests to ensure it is performing its cryptographic functions correctly. If any of these checks fails, the device will halt and require Network Administrator intervention to successfully start-up.

g. TOE access

The TOE can be configured by the Network Administrator to set an interactive 'session timeout' value (any integer value in minutes and also optionally in seconds, with 0 disabling the timeout) – the default timeout is 10 minutes. A session that is inactive (i.e., no commands issuing from the remote client) for the defined timeout value will be terminated.

The user will be required to re-enter their user id and password, so they can be re-authenticated in order to establish a new session. The TOE can be configured to display administrator-configured advisory banners that will be displayed in conjunction with user login prompts. The banner contents are configured by a user in the role of Network Administrator role.

h. Trusted Path/Channels

To support secure remote administration, the TOE includes implementations of SSHv2 and SNMPv3. In each case, a remote host (presumably acting on behalf of an administrator) can initiate a secure remote connection for the purpose of security management. Note that only the local console is available by default and each of these remote administration services can be independently enabled by a Network Administrator.

In the case of SNMPv3, the TOE acts as a SNMPv3 server accepting non-interactive Management Information Base (MIB) options from an authenticated source. SNMPv3 requires the client to be authenticated against a locally configured user base and utilizes AES-128 in order to protect this security management channel.

B 7.3 Vulnerability Analysis and Penetration testing

In search of potential vulnerabilities, the evaluator has conducted public domain search, focusing on the type of the TOE. The listed vulnerabilities in the public domain for this type of TOE were analyzed and filtered list was prepared with those which are applicable for the type of TOE under consideration (i.e. router).

The TOE documents like, Security Target (ST), TOE architecture & Design (TDS), TOE Preparatory guidance document etc. were analyzed to find out potential security vulnerability and the same is listed in.

The attack potential for each of the vulnerabilities was calculated using guidance given in CEMv3.1 and considering various factors like the time to identify & exploit the vulnerability, expertise required, knowledge of the TOE, windows of opportunity and equipment requirement.

Subsequent to the independent review of public domain vulnerability databases and all evaluation evidences, potential vulnerabilities were identified with their attack potentials. The potential vulnerabilities with '**Basic**' attack potential were considered for penetration testing.

The potential vulnerabilities with higher than 'Basic' attack potential are treated as residual vulnerabilities.

Penetration testing scenarios are summarized as below:

- Escalation of privileges that should otherwise be denied
- Bypassing ACL during booting up
- Unauthorized access of management plane through data plane traffic
- Running of untrusted software on the TOE
- Disturbing TSF behavior through flooding the TOE with TCP malformed packets
- To make TOE log unavailable while transporting the same to external log server
- To make external Authentication service unavailable.

The penetration testing could not exploit any vulnerability in the intended operational environment of the TOE. However, these vulnerabilities may be exploited with higher attack potential.

B 9 Evaluation Results

The evaluation results have been documented in the [ETR].

The TOE was evaluated through evaluation of its documentation, site visit, testing and vulnerability assessment using methodology stated in [CEM] and laboratory operative procedure [OP-07].

Documentation evaluation results:

The documents for TOE and its development life cycle were analyzed by the evaluator in view of the requirements of the respective work units of the [CEM]. The final versions of the documents were found to comply with the requirements of CCv3.1 for EAL3.

Site Visit:

Evaluator has analyzed requirements for site visit and found that the developer's configuration management system, delivery procedure and security measures in development area are complying with the requirements of CCv3.1 for EAL3.

Testing:

The developer's tests and the independent functional tests yielded the expected results, giving assurance that 'Comware V7.1.049 running on MSR2000, MSR3000, and MSR4000 Series Routers router hardware'

behaves as specified in its [ST], functional specification and TOE design.

Vulnerability assessment and penetration testing:

The penetration testing with '**Basic**' attack potential could not exploit the potential vulnerabilities identified through vulnerability assessment.

B 10 Validator Comments

The Validators have reviewed the Evaluation Technical Report [ETR] along with all relevant evaluation evidences, documents, records, etc. and are in agreement with the conclusion made in it i.e.

- **The [ST] has satisfied all the requirements of the assurance class ASE.**
- **The results of evaluation of product and process documentation, site visit report, testing and vulnerability assessment confirm that 'Comware V7.1.049 running on MSR2000, MSR3000, and MSR4000 Series Routers router hardware', satisfies all the security functional requirements and assurance requirements as defined in the [ST]. Hence, the TOE is recommended for EAL3 Certification**.

However it should be noted that there are no **Protection Profile** compliance claims.

B 11 List of Acronyms

ACL: Access Control List
CC: Common Criteria
CCTL: Common Criteria Test Laboratory
CEM: Common Evaluation Methodology
DVS: Development security
EAL: Evaluation Assurance Level
ETR: Evaluation Technical Report
FSP: Functional Specification
IC3S: Indian Common Criteria Certification Scheme
IT: Information Technology
PP: Protection Profile
ST: Security Target
TOE: Target of Evaluation
TDS: TOE Design Specification
TSF: TOE Security Function
TSFI: TOE Security Function Interface

B 12 References

1. [CC-I]: Common Criteria for Information Technology Security Evaluation: Part 1: Version 3.1
2. [CC-II]: Common Criteria for Information Technology Security Evaluation: Part 2: Version 3.1
3. [CC-III]: Common Criteria for Information Technology Security Evaluation: Part 3: Version 3.1
4. [CEM]: Common Methodology for Information Methodology: Version 3.1
5. [ST] : Hewlett-Packard Company Comware V7.1 Running on MSR2000, MSR3000, and MSR4000 Series Routers Security Target, version 0.11
6. [ETR]: Evaluation Technical Report No. STQC IT (KOL)/STQC/CC/1415/15/ETR v 1.0
7. [OP-07]: CCTL operating procedure