Indian CC Certification Scheme (IC3S)

Certification Report

Report Number	**:**	**STQC/CC/14-15/12/CR**
Product / system	:	**CROS-1.8.22-S01 Software running on C-DOT CRAT-100/CRDT-100 Router**

Dated: 23rd June 2020

Version: 1.0

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

Product developer:	Centre for Development of Telematics (C-DOT), India
TOE evaluation sponsored by:	Centre for Development of Telematics (C-DOT), C-DOT Campus, Mandi Road, Mehrauli, New Delhi 110030
Evaluation facility:	Common Criteria Test Laboratory, ERTL (East), Block DN 63, Sector V, Salt Lake, Kolkata-700091, India.
Evaluation Personnel:	**Evaluators:** Malabika Ghose, Sc. F & Manikanta Das, Sc. F **Test engineers:** Nischal & Aniruddha Ghosh
Evaluation report:	Report No: STQC/CC/14-15/12/ETR/0017
Validation Personnel:	Subhendu Das, Scientist G

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	*Centre for Development of Telematics (C-DOT), C-DOT Campus, Mandi Road, Mehrauli, New Delhi 110030*
Developer	*Centre for Development of Telematics (C-DOT), C-DOT Campus, Mandi Road, Mehrauli, New Delhi 110030*
The Target of Evaluation (TOE)	*The TOE is identified as '**CROS-1.8.22-S01 Software running on C-DOT CRAT-100/CRDT-100 Router**'.* *It is a Routing Operation System software (CROS-1.8.22-S01) running on CRAT-100/CRDT-100 routing platform providing routing/switching functionality in IP/MPLS network. The TOE receives network packets from source network nodes to its physical ports, processes them and forwards them to destination port based on available routing information. This routing information is either dynamically calculated by TOE or configured by TOE users.*
Security Target (ST)	***'Security Target For C-DOT CRAT-100 / CRDT –100 Router Running CROS-1.8.22-S01 Software, Version 07'***
Brief description of product	*The TOE is a software (identified as 'CROS-1.8.22-S01'), running within the physical boundary of CRAT-100/CRDT-100 system which is a single card routing platform having network data and management interfaces. The system supports both routing and switching functionality. The TOE can be configured through Command Line Interface (CLI) over SSH connection. It can be synchronized with NTP server. The user authentication for remote login can also be done through external RADIUS/TACACS server. The system logs can be transferred to external syslog server from time to time.* *CRAT-100 and CRDT-100 routing platforms are equivalent, in terms of their hardware, except their power supply. CRAT-100 is an AC powered (220V) system whereas CRDT-100 is powered through DC power (-48V) supply. The AC and DC power supply modules are interchangeable in the system. The hardware functionality and the CROS software functionality run on these platforms are independent of their power supplies (AC or DC).*
CC Part 2 [CC-II]	*Conformant*
CC Part 3 [CC-III]	*Conformant*
EAL	*EAL 3*
Evaluation Lab	*ERTL(E)-CCTL: Common Criteria Test Laboratory, ERTL (East), Block DN 63, Sector V, Salt Lake, Kolkata-700091, India*
Date Authorized	*8.01. 2019*

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 BS7799/ISO27001 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, the then, Department of Information Technology (now MeitY), STQC Directorate to evaluate & certify the trustworthiness of the security features in Information Technology (IT) products and systems. IC3S, Indian Common Criteria Certification Scheme, is an independent third-party certification scheme for the security functions or mechanisms of the IT products. It also provides framework for 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) IC3S, the Certification Body, operated by STQC, Dte., Min. of Electronics and Information Technology, 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), Block DN 63, Sector V, Salt Lake, Kolkata-700091, West Bengal, India. Hereafter this is referred as '**ERTL (E)-CCTL**'. The evaluation facility is recognized under Indian Common Criteria Certification Scheme (the IC3S).

Centre for Development of Telematics (C-DOT), C-DOT Campus, Mandi Road, Mehrauli, New Delhi 110030, India is the developer of the product and as well as is the sponsor of the TOE evaluation.

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

The evaluation team completed all task on 8th June 2020 and handed over the Evaluation Technical Report [ETR] to the validator (on behalf of the certification body).

The confirmation of the evaluation assurance level (EAL) applies on the following conditions:

- 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 with its guidance documents, indicated here. The validity of the certificate can be extended to cover new versions and releases of the product, provided the developer /sponsor of the product applies for assurance continuity/re-certification for the modified product, in accordance with the procedural requirements.

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 https://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 the TOE. It presents the evaluation results and the conformance results. This certificate report 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 the CC Evaluators of ERTL(E)-CCTL. The information, presented in this report, are derived from the [ST] written by the developer and the Evaluation Technical Report [ETR] issued by Common Criteria Test Laboratory [ERTL (E)-CCTL]. The evaluation team determined the product is conformant to Common Criteria Standard, ver. 3.1, following Common Evaluation Methodology [CEM] and concluded that the Target of Evaluation meets the requirements for Evaluation Assurance Level (**EAL 3**) of the Standard.

B 1.2 Evaluated product and TOE

The **Software, CROS-1.8.22-S01,** identified as **TOE** is **running on CRAT-100/CRDT-100 routing platform** providing routing/switching functionality in IP/MPLS network. It receives network packets from source network nodes to its physical ports, processes them and forwards them to destination port based on available routing information. This routing information is either dynamically calculated by TOE or configured by TOE users. The TOE is intended to protect the User's data and the TOE data which provides network services to the users.

The **CRAT-100/CRDT-100 system** is designed to address Core and Edge layer of typical IP/MPLS network deployment. This system can be used as routing solution for a broad range of applications in the datacenter and in 'Service Provider's' environments. The CRAT-100/CRDT-100 system can act as a standalone L2-L4 switching and routing system for converged Ethernet datacenters, as well as broadband aggregation systems. CRAT-100/CRDT-100 system supports both routing and switching functionality. The required features on devices can be configured using software driven management interface. So, same device can work as an L2 switch, L3 Switch, or router, as required by the user. It implements industry standard compliant Operations, Administration and Management features to manage the network. It provides standard compliant software/hardware interfaces for interoperability.

CROS-1.8.22-S01 software has distributed architecture with clear separation of Forwarding Plane processing from the Control Plane processing. Similarly, both the Forwarding Plane and the Control plane are decoupled from the management plane ensuring TOE protection. During startup, TOE performs a series of self-tests which checks the integrity of the TOE. In case of fault, TOE fault management (FM) feature handles and recovers the fault, providing the uninterrupted services of system.

CRAT-100 and CRDT-100 platforms are equivalent in terms of their hardware except their power supply. CRAT-100 is an AC powered (**220V**) system whereas CRDT-100 is powered through DC power **(-48V**) supply. The AC and DC power supply modules are interchangeable in the system. The hardware functionality and the CROS software functionality run on these platforms is independent of the power supplies (AC or DC).

The evaluated version of the product, with its guidance documents, have been described as the Target of Evaluation (TOE) in this report. The Evaluated Configuration of the product, its security functions, assumed environment 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 3.2 and 4.1 of ST). All the Security Functional Requirements (SFRs), listed in 6.2 of [ST] are taken from CC Part 2. **The threats** considered by the developer are as below:

i. An unauthorized entity may disrupt the TOE operation or hamper its security mechanism, so that it can interrupt the network data flow.

ii. An unauthorized user may get access to TOE security functions and data to disrupt the security function of TOE by changing the configuration data.

iii. An unauthorized process or application may get access to TOE security functions and data to disrupt the security function of TOE by changing the configuration data.

iv. Network traffic may be intercepted and unauthorized changes to management traffic from or to the TOE may be done.

v. Failure of network components may lead to loss of configuration data which may not be restored immediately

vi. Unauthorized changes to the TOE configurations and other management information may not be detected

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/14-15/12 dated 22nd July 2014, however, CDOT issued the work order to the Evaluation Facility in March 2016.

The TOE as described in the [ST] is "**CROS1.8.22-S01 Software running on C-DOT CRAT-100/CRDT-100 Router**". receives network packets from source network nodes to its physical ports, processes them and forwards them to destination port based on available routing information. This routing information is either dynamically calculated by TOE or configured by TOE users. The TOE was evaluated through assessment of its Architecture, design and Development documentation, Testing of Security functions, Review of source codes responsible for rendering Security Functions and Focused Vulnerability Assessment, using methodology stated in Common Evaluation Methodology [CEM] of CC Standards and Operating Procedure, OP-07 of Common Criteria Test Laboratory, ERTL (E), Kolkata.

The evaluation has been carried out under written agreement [6th March 2017] 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.

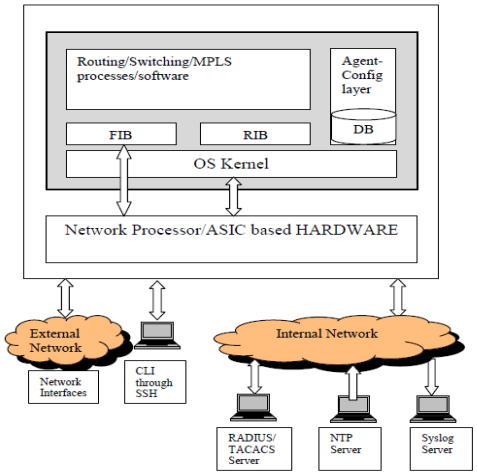
B 1.7 Recommendations and conclusions

- 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.

B2 Identification of TOE

CROS-1.8.22-S01 software running within the physical boundary of CRAT-100/CRDT-100 system which is a single card

routing platform having network data and management interfaces. The TOE can be configured through Command Line Interface (CLI) over SSH connection. It can be synchronized with NTP server. The user authentication for remote login can also be done through external RADIUS/TACACS server. The system logs can be transferred to external syslog server from time to time. The architectural block diagram of the TOE is shown below:



TOE environment:
The intended operational environment for the evaluated TOE is C-DOT CRAT-100/CRDT-100 system

Non-TOE Environment:

1. External authentication services will be available via RADIUS.
2. External NTP services will be available.

Delivery to the user

Following are the parts/items delivered to the TOE user:

S. N	Part/Item Description	Delivery method
1.	CRAT-100/CRDT-100 Router Hardware along with 2 set of power cable, one USB to Serial Cable and Hardware Release Note	Packed in box and shipped by post
2.	CROS-1.8.22-S01 with Software Release Note	In a CD and shipped by post
3.	Installation Manual-v07	In a CD and shipped by post
4.	User Manual-v05	In a CD and shipped by post

B3 Security policy

There are no organizational security policy (ies) that the TOE is expected to meet.

B.4 Assumptions

There are following assumptions exist in the TOE environment.

Table 1: Assumptions

A. Type	Description
A.ACCESS	The TOE will be located within controlled access facilities, which will prevent unauthorized physical access to TOE.
A.COMP_NOEVIL	The authorized users of TOE will be trained and competent to use TOE, and not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

A.EXTAUTH	External authentication services will be available via RADIUS.
A.TIME	External NTP services will be available.
A.NWCOMP	The network components that access the management interface of the TOE will be located within a controlled and secure environment. The authorized users of the components will not be willfully negligent or hostile.
A.LIMITED_FUNCTIONALITY	The TOE is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general-purpose computing. For example, the device should not provide computing platform for general purpose applications (unrelated to networking functionality).
A.NO_THRU_TRAFFIC_PROTECTION	A standard/generic network device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the TOE to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the TOE, destined for another network entity, is not covered by this ST. It is assumed that this protection will be covered by for particular types of network devices (e.g. firewall).

B.5 Evaluated configuration

CROS-1.8.22-S01 Software running on CDOT CRAT-100 / CRDT - 100 Router (build #2920) consists of the following files

i. **The TOE (Product):** CROS-1.8.22-S01 Software components

cDotDPSrvr: is the Data Plane binary file: eba2448a672f50b073bd581ba4b0f055 (MD5)
cDotCPSrvr: is the Control Plane binary file: 837576400efb8d153ad0649e4cc63353(MD5)
cDotFMSrvr: is the Management Plane binary file: 3a7225c5aca467ec2a09facf8360fac3(MD5)

ii. **TOE Environment:**

a) Hardware

CRAT100/CRDT-100 routing platform.

CRAT-100 and CRDT-100 platform are equivalent in terms of their hardware except their power supply. CRAT-100 is an AC powered (220V) system whereas CRDT-100 is powered through DC power (-48V) supply. The AC and DC power supply modules are interchangeable in the system. The hardware functionality and the CROS software functionality run on these platforms is independent of the AC or DC power supplies.

b) Software (the TOE and its associated software environment)
The package containing TOE executables having following hash values (MD5).

52e7ceaa888ba5f67ace792b18abe9ce	core-rootfs-v1.8.22-s01.tar.bz2
4d91c6f93900ba93c0e874e3aba6ca25	core-rootfs-v1.8.22-s01.tar.bz2.md5sum
c42ab3f8633e32f558e3eac8edab5ed9	ubootScript-v1.8.22-s01.img
583e76328d241a89de6c4047cefe1e3d	uImage-initramfs-v1.8.22-s01.bin
fefd49ef310ad20d0406f3644a6cf3cd	uImage-initramfs-v1.8.22-s01.bin.md5sum
98a50d0639c67fa2f92b04634cb87842	u-boot. bin

B6 Document Evaluation

B.6.1 Documentation

The list of documents, presented, as evaluation evidence to the evaluation team are given below:

1. **Security Target**: Developer's doc/ artefact: 'Security Target For C-DOT CRAT-100/CRDT-100 Router Running CROS-1.8.22-S01 Software'

i. Document Identification: CDOT-NGN-ST-CROS-v07 d03
ii. Version: 07
iii. Date of release: 06.02.2020

2. **TOE Architecture:** Security Architecture For C-DOT CRAT-100/CRDT-100 Router Running CROS-1.8.22-S01 Software Version 05 (CDOT-NGN-ARC-CROS), version 05
3. **TOE Functional Specification:** Functional Specification For C-DOT CRAT-100/CRDT-100 Router Running CROS-1.8.22-S01 Software (CDOT-NGN-FSP-CROS), version 07
4. **TOE Design description**: TOE Security Design For C-DOT CRAT-100/CRDT-100 Router Running CROS-1.8.22-S01 Software (CDOT-NGN-TDS-CROS), version 04
5. **TOE Preparative Guidance**:
   Router Installation Manual CDOT-NGN-MAN-INSTALL-CROS Version 05
6. **TOE Operational Guidance**:
   Router User Manual CDOT-NGN-MAN-USR-CROS Version 04
7. **TOE Configuration Management Capability:** Configuration Management Plan for C-DOT CRAT-100/CRDT-100 Router Running CROS Software ver. 04
8. **TOE Configuration Management Scope:** Configuration Management Plan for C-DOT CRAT-100/CRDT-100 Router Running CROS Software ver. 04
9. **TOE delivery Procedure:** Configuration Management Plan for C-DOT CRAT-100/CRDT-100 Router Running CROS Software ver. 04
10. **TOE development and maintenance life-cycle model:** Configuration Management Plan for C-DOT CRAT-100/CRDT-100 Router Running CROS Software ver. 04
11. **Test cases, logs, and coverage**:
    CDOT-NGN-FTC-CROS-V01-v03.pdf and CDOT-NGN-FTC-CROS-V02-v03.pdf

B.6.2 Analysis of document

The documents related to the following areas were analyzed following the guidance stated in respective Work Units of Common Evaluation Methodology, ver. 3.1[CEM]. The summary of analysis is as below:

The ST:

The evaluation team checked, analyzed the ST document, presented for the TOE, and confirmed that ST complies all requirements of the Common Criteria Standards, ver. 3.1 and internally consistent. The TOE provides following security features:

1. User Data Protection
2. Identification and Authentication
3. Security Management
4. Audit
5. TOE Access Function
6. Protection of TOE Security Functions (TSF)
7. Cryptographic Support

The intended operational environment for the evaluated TOE assumes that:

1. External authentication services will be available via RADIUS.
2. External NTP services will be available.
3. The network components that access the management interface of the TOE will be located within a controlled and secure environment.
4. The authorized users of the components will not be negligent or hostile.
5. The TOE is assumed to provide networking functionality as its core function and not provide

functionality/services that could be deemed as general-purpose computing.

6. Traffic that is traversing the TOE, destined for another network entity, is not covered by this ST. The intent is for the TOE to protect data that originates on or is destined to the device itself, to include administrative data and audit data. It is assumed that this protection will be covered by for types of network devices (e.g. firewall)

TOE Development (Functional Specification, Architecture, and Design):

Functional Specification:

The evaluation team analyzed the functional specification of the TOE in consultation with TOE Design, Guidance document, TOE implementation document and found that the TOE security function interfaces are described clearly and unambiguously.

Security Architecture description:

The evaluation team analyzed the descriptions of the Security Architecture of CROS-1.8.22-S01 Software and confirmed that the TSF maintains the ***security domains*** as follows:

The four constituents of the C-DOT Terabit Router **Control Plane**, **Data Plane**, **Management Plane** and **System Software** are separated with each other according to their functionalities. These constituents run as separate Linux Process and interact with each other with well-defined interfaces. Hence, during the boot-up of the router or during the user configuration of any one of the constituents cannot be corrupted on the failure of the others. The software responsible for realization of **Control Plane**, **Data Plane and Management Plane** functionalities are stored under Linux file system and protected by the Operating System. The TOE software is protected from any access (read/write) from its users, except from Linux root who can login, only from the system console. So, no one can modify or delete any of the router security function or any other routing functions.

The evaluator also confirmed that the TSFs are getting ***initialized securely*** as below:

The various sub-systems of the TOE coupled with the security functions have a well-defined start-up process. On power-on or re-boot, TOE self-test is performed. During self-test, the integrity of Control Plane, Data Plane and Fault Management Plane binaries are checked, sequentially. If self-test is passed, the routing application software is loaded, i.e. Management Plane, Data Plane, Control Plane and Fault Management Plane of the TOE are loaded. The last active configuration or factory default attributes is initialized and the TSFs are initialized.

TSFs are **architecturally protected** in this TOE, through the following means:

The TOE protects its security functions through various mechanisms. It performs self-test to verify the integrity of the application software and ensures that the application software is not tampered with before it is loaded. During integrity check, it calculates the HASH value of the software files and compares it with the respective stored HASH value of each of the software files. In case of failure in integrity check, the router application software is not loaded onto the system and router goes into a fail secure mode. If integrity check is passed, it loads the router application software and initializes TOE with last active configuration file or with factory setting attributes and brings the router to a known stable state. The factory default file initializes all the interfaces of the TOE with the default parameters, such as interface name, type, speed, MTU.

Bypassing the SFR-enforcing functionalities is **prevented architecturally**:

The TOE is accessible to its user only when all the sub-systems of the router are booted properly and in the well-defined order. None of the functionality of the TOE is accessible until all the sub-system boot up and working properly. The Access Control functionality is implemented in the management plane of the router. The router provides both 'In-Band' as well 'Out-of-Band' management. User can only access the router through its management port, using SSH. Once authenticated, user gets access to Command Line Interface (CLI). Users can run any of the commands through CLI, as per authorization given to them which depends on the associated User Role. The access to management plane is also protected through management plane ACL. An authorized user can login to management plane (In-Band or Out-of-Band management), if and only if, its client IP Address is permitted in the management ACL, which can only be configured by Root-System. In case of In-Band management, an authorized user can login to Router Data port to manage the Router provided user client IP-Address is permitted in the management ACL which can again be configured by Root-System.

Design description:

The description of the TOE has been made in terms of sub-systems and modules. The TOE comprises of nine software sub-systems, viz, TOE Initialization, TOE Access, SSH & Cryptographic Support, Identification & Authentication, Network Traffic Flow Control, TOE Rollback, TOE Configuration Data, Audit and Monitor TOE Configuration.

Each subsystem has been further described in terms of modules. The Evaluator analyzed the mapping of the modules with the subsystems, their interactions and traceability to the SFRs (in Security Target) and the TSFIs (in the Functional Specification) to arrive into the conclusion about the correctness of the design document.

Guidance Documents: The evaluators analysed guidance documents like preparative procedure and operational user guidance and determined that preparative procedure describes clear and unambiguous steps to bring the TOE to its secure state. The operational user guidance information is also 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 virtual site visit. The end-users can check integrity of the evaluated TOE using hash value of that, if felt necessary.

The final versions of the respective evaluation evidences are found to comply with the requirements of CCv3.1 for EAL 3.

B7 Product Testing

Testing at EAL 3 consists of the following three steps:

i. Testing by developer

ii. Independent Testing by Evaluation Team, and

iii. Penetration testing.

B 7.1 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 analysed 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 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:

Evaluator planned for 16 test cases, covering ALL the TSFIs and the SFRs (Security Functional Requirements) sated in ST. The tests were conducted in an environment, which is consistent with the Operational Environment of the TOE, declared in the ST. All the tests have successfully passed.

B 7.3 Vulnerability Analysis and Penetration testing

The evaluator used scanning tools to identify publicly known vulnerabilities as these standard tools include attack scripts covering type of the TOE, technology and OS used. A scanning has been conducted on the TOE with plugin set (202003232053) of the tool 'nessus' to find out presence of hypothesized potential vulnerabilities, identified in the public domain, pertaining to this type of product. The results of vulnerability scanning tool 'nessus' (with plugin set 202003232053) did not reveal any vulnerabilities which are known in the public domain.

The evaluator has analyzed the evaluation evidences like, the ST, the Functional Specification, the TOE Design, the Security Architecture Description and the Guidance Documentation and as well as the operational environment, stated in the ST and then hypothesized the security vulnerabilities considering five categories of attack to the Security functions, viz. 'Bypassing', 'Tampering', 'Direct Attacks', 'Monitoring' and 'Misuse'.

Considering the type of the TOE and its intended use (TOE can be accessed by Authenticated users only), the possibility

of "Direct Attack" is negligible. The evaluator has further justified this conclusion by considering the TOE feature of account locking (on consecutive unsuccessful login attempts). The Evaluator's judgement is justified and supported by analysis.

The evaluator has analyzed the TOE and other evaluation evidence for possibility of other types of attacks, like 'Bypassing', 'Tampering', 'Monitoring' and 'Misuse' and arrived in following Attack scenarios.

Category Bypass:

AT 1. Attacker may access network resources, which are not within its privileges if data plane starts transmitting packets before control plane is loaded.

Category Tampering:

AT 2. The attacker may tamper weakly encrypted password to gain illegitimate access to the TOE.

AT 3. Attacker may exploit the scenario that the TOE cannot handle heavy traffic in the data port and behave erratically.

Category Monitoring:

The Security target (ST) document assumes that the TOE communicates with external IT entities like RADIUS / TACACS / SYSLOG / NTP, through trusted channel (OE.EXT_AUTH and OE. TIME_SYNC).

Additional effort by the evaluator:

During the evaluation process, the TOE was modified and finally achieved requisite compliance. Time to time the feedbacks from the evaluation team have facilitated the developer to improve the security of the TOE. The developer has rectified this vulnerability in the final version (ver.1.8.22-S01) of the TOE.

Considering hypothesized vulnerabilities and associated attack scenarios of AT1, AT2 and AT3, the evaluator estimated the respective attack potentials, following the guidelines of CEMv3.1. The estimated attack potentials for AT1 & AT2 are found to be more than 'Basic' and hence not considered during Penetration Testing.

As the target assurance level is **EAL 3**, the evaluation team has restricted their Penetration Testing activities with 'used attack potential' of 10 (more than 'Basic' Attack Potential),.The Penetration testing conducted by the Evaluation team at Developer's premises using their Spirent Test Centre. All 48 data ports are loaded with 10G Traffic, and management port is accessed to observe TOE behaviour. The evaluator didn't find any abnormal behaviour the Security function of the TOE. Hence, it is concluded that the TOE does not contain any exploitable vulnerability for '**Basic'** Attack Potential. Considering the fact that all security measures can be broken, if the time and resource to the attacker are unlimited, this TOE may have some security weakness which can be exploited with the attacks having higher attack potential than 'Basic'.

The Evaluator has identified such vulnerabilities and declared them as residual vulnerabilities for this Security Evaluation. The reported residual vulnerabilities are as follows:

1. Attacker may somehow disturb the booting process of the TOE and force its data plane to start packet transmission before control plane is properly loaded. This may lead to give access to network resources which are not within its privileges.
2. The attacker may break the encryption of the password and gets illegitimate access to the TOE

B 9 Site visit

The Evaluation team visited developer's site at CDOT, New Delhi on 24/02/2020, 25/02/2020 and 26/02/2020 in connection with Common Criteria EAL 3 evaluation of the Target of Evaluation (TOE). The objectives of site visit were to confirm specific requirements of the CC standards related to CM system used for TOE development, delivery procedure of the TOE and Security of the TOE development environment.

The Evaluation team has drawn their satisfactory conclusion after the site visit and confirmed that the specific requirements for EAL 3 are met in respect of ALC_CMC.3, ALC_DEL.1 and ALC_DVS.1.

B 8 Evaluation Results

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

The TOE was evaluated through evaluation of its documentation, 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.

Testing:

The developer's tests and the independent functional tests yielded the expected results, giving assurance that '**CROS1.8.22-S01 Software running on C-DOT CRAT-100/CRDT-100 Router**', 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 9 Validator Comments

The Validators have reviewed the Evaluation Technical Report [ETR] along with all relevant evaluation evidence, documents, records, etc. and are in agreement with the conclusion made in it, which are as follows:

- **The [ST] has satisfied all the requirements of the assurance class ASE.**
- **The results of evaluation of product and process documentation, testing and vulnerability assessment confirm that 'CROS1.8.22-S01 Software running on C-DOT CRAT-100/CRDT-100 Router', satisfies all the security functional requirements and assurance requirements as defined in the [ST]. Hence, the TOE is recommended for Common Criteria EAL 3 Certification**.

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

B 10 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 11 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]: C-DOT CRAT-100/CRDT-100 Router Running CROS-1.8.22-S01 Software'
    i. Document Identification: CDOT-NGN-ST-CROS-v07d03
    ii. Version: 07
    iii. Date of release: 06.02.2020
6. [ETR]: Evaluation Technical Report On CROS-1.8.22-S01 Software running on CDOT CRAT-100 / CRDT 100 Router, Report No: STQC/CC/14-15/12/ETR/0017
7. [OP-07]: CCTL operating procedure