IC3S

Guidance for Vulnerability Assessment of TOE
(STQC/CC/D18)
Issue : 01

CC Certification Body, STQC Directorate,
Indian Common Criteria Certification Scheme (IC3S),
MeitY,Government of India
INDIA

Table of Contents

0.1 Approval and Issue

Reviewed by : Management Representative

Approved by : Head, CC Scheme

Note:

- Management Representative is responsible for issue and distribution of this document including amendments.
- Holder of this copy is responsible for incorporation of all the amendments and currency of the document.

0.3 Amendment Record

Sl. No.	Date	Issue	Reason of Change / Change Details
1.	30-09-20	01	First Issue

1.0 Purpose

This document describes the procedure for conducting vulnerability analysis (AVA_VAN) of the TOE in CC Test Laboratory (CCTL). Vulnerability analysis includes assessment of exploitability of flaws or weaknesses of TOE in operational environment. This assessment is based on analysis of evaluation evidences and related publicly available materials followed by penetration testing.

2.0 Scope

The scope of this procedure is limited to the vulnerability analysis activities taken up by CCTLs, for evaluation as per the requirements of Common Criteria standards, up to EAL4.

3.0 Definitions

For the purpose of this document, the terms, definitions, symbols and abbreviated terms given in section 4 & 5 of [CC-Part1] and [CEM] shall be applicable.

4.0 Reference Documents

[CC-Part1]: Introduction and general model

[CC-Part2]: Security functional components

[CC-Part3]: Security assurance components

[CEM]: Common methodology for information technology security evaluation ISO/IEC 15408-Part I to III: Common criteria for Information technology.

(Please refer Master List of Documents for latest version of the documents)

5.0 Input

CCTL shall formally undertake AVA_VAN after receiving the following inputs from the developer.

- TOE specific documents like ST, functional specification, TOE design, security architecture description, implementation representation, Guidance etc. as per the requirements of [CC-Part3] and commensurating with the targeted EAL
- TOE suitable for testing at its final version.

6.0 Responsibilities

The designated evaluator for the specific project shall be responsible for following activities:

- Identification of hypothesized potential vulnerabilities of the TOE from public domain
- Identification of hypothesized potential vulnerabilities of the TOE from evaluation evidences
- Estimation of attack potential of all identified hypothesized potential vulnerabilities
- Conducting penetration testing of all hypothesized potential vulnerabilities having attack potential less than or equal to the targeted withstandable attack potential of the TOE.
- Preparation of Observation Report [OR] in case of any anomaly / exploitable vulnerability revealed in the TOE during penetration testing
- Identification of exploitable and residual vulnerabilities of the TOE
- Preparation of Vulnerability Assessment report addressing the requirements of CC part-3 and CEM
- Preparation for necessary inputs for ETR as per requirement of [CEM]

Head of the CCTLs shall be responsible for following activities:

- Review and approve Observation Report [OR]
- Review and approve the vulnerability assessment report.

7.0 Detailed Procedures

7.1 Identification of hypothesized potential vulnerabilities of the TOE from public domain

The evaluator shall search publicly available information for published vulnerability for a specific type of TOE. The public domain includes books, magazines, research papers, web-sites etc. The test manager shall remain open to consider any other types of resources for the purpose. The vulnerability information which is easily available to the test manager is also available to the attacker leading to lower the attack potential value. These points are to be considered during estimation of attack potential for any potential vulnerabilities. All collected relevant vulnerabilities shall be noted down. These collected vulnerabilities shall be documented. Then each shall be analyzed whether it may be present in the TOE or not. Technical justification must be recorded for whether or not the specific vulnerability will be considered further. For example, while evaluating a router OS, vulnerabilities related to all other similar OS will be considered first. Then, one by one, each vulnerability will be analyzed whether it or its type can be present in the current TOE. Any doubt must lead to the inclusion of the vulnerability as one of the potential vulnerabilities.

7.2 Identification of hypothesized potential vulnerabilities of the TOE from evaluation evidences

The evaluator shall search evaluation evidences like ST, Functional Specification, Architecture, Design document, Guidance document etc., as applicable for a specific EAL, to find out areas of concern. These areas of concern will be analyzed whether these are leading to any potential vulnerabilities within TOE. If potential vulnerabilities are identified, then, those may be categorized under bypassing, tampering, direct attacks, monitoring and misuse. A methodical approach to analyse threats, security objectives and security functions would be considered. Each security function along with its interfaces would be analyzed whether it adequately meets the relevant security objectives and address the threats. Then, it would be judged whether the identified potential vulnerabilities are present in the operational environment of the TOE considering all security functions are implemented properly. Then, these identified potential vulnerabilities shall be documented.

7.3 Estimation of attack potential of all identified hypothesized potential vulnerabilities

The evaluator shall consider attack scenarios for each of those potential vulnerabilities identified in step 7.1 and 7.2 during estimation of attack potential. Attack potential for any vulnerability gives a measure of amount of effort to be spent to create the attack.

The factors which will be considered during attack potential estimation are as follows:

a. Time taken to identify and exploit (Time Elapsed)
b. Technical expertise required (Expertise)
c. Knowledge of the TOE design and operation (Knowledge of TOE)
d. Window of opportunity
e. Equipment required

Calculation can be done based on guidelines given in CEM and using the template given in Annexure – I.

7.4 Conducting Penetration testing of all hypothesized potential vulnerabilities having attack potential less than or equal to the targeted resistant attack potential of the TOE

7.4.1 Test Environment:

The penetration testing has to be carried out in an isolated network simulating target environment as far as possible as stated in the Security Target document (ST) for the specific TOE. The TOE shall be made available at its final version (for evaluation). If ST specifies more than one configuration for the TOE, then each of the configurations shall be considered for the penetration testing.

7.4.2 Test Preparation:

All identified potential vulnerabilities which have attack potential equal to or less than the targeted attack potential will be subjected to penetration testing. Series of test cases may be designed for each of these potential vulnerabilities. The TSFIs invoked to resist each of theses potential vulnerabilities are to be identified. Test procedure and required test equipments are also to be identified and documented. These information may be documented using the template given in Annexure – II.

7.4.3 Execution of testing:

The evaluator shall conduct testing based on documentation prepared in the step 7.4.2.

7.4.4 Recording test results:

- Actual test results are to be recorded for each test case. These may be recorded using template given in Annexure –II.
- If actual test result deviates from expected test result, then an anomaly will be indicated which in turn will be reflected in OR.
- The anomalies, if found, will be communicated to the developer.

7.5 Preparation of Observation Report [OR] in case of any anomaly

If the TOE fails in penetration testing, then the failure report shall be sent to the developer in the form of Observation Report (OR). The developer will then resubmit the TOE after correction along with all relevant documents. The evaluator will repeat relevant independent testing and penetration testing.

7.6 Identification of residual vulnerabilities of the TOE

The potential vulnerabilities which are not considered for penetration testing shall be listed as residual vulnerabilities.

7.7 Preparation for necessary inputs for ETR as per requirement of [CEM]

- The evaluator shall report in the ETR the penetration testing effort, outlining the testing approach, configuration, depth and results.
- The evaluator shall also report in the ETR all residual vulnerabilities.

Annexure - I

Template to Calculate attack potential of hypothesized potential vulnerabilities
VS1. Title of the vulnerability

Factor	Effort for Identification and Exploiting the vulnerabilities (ref Table 3 of Annex B, CEMv3.1)	Remarks
Time Elapsed(a)		
Expertise(b)		
Knowledge of TOE(c)		
Window of opportunity(d)		
Equipment(e)		
Attack potential Σ(a+b+c+d+e)		

Annexure - II

Template for penetration testing of potential vulnerabilities with 'xxx' attack potential level

Vulnerability No	:	
Vulnerability Detail	:	
Test Equipment	:	
Test Procedure	:	
Execution of the test	:	
Expected Result	:	
Actual Result	:	
Remarks	:	
Post processing	:	