Swedish Certification Body for IT Security
Scheme Note 22 - Vulnerability assessment

Scheme Note

Decision Date	Matter ID	
2020-11-19	CR-3016 (CR-2802, CR-2589, CR-2470, CR-2354)	
Decision by (Name/Title)	Scheme Note Number	Dnr
Dag Ströman, Head of CSEC	22	nXnn
Presentation by	Present at the Meeting	
Jerry Johansson	CCB 2020-11-19	

Schematolkningens innebörd/Scheme Note Statement

Description and References

Background

This Scheme note relates to four issues regarding vulnerability assessment.

Methodology for vulnerability database search

The vulnerability database search is becoming a more and more important part of the vulnerability assessment. In order to facilitate the certifier's review of the vulnerability assessment, the evaluators should follow the basic methodology described below. The evaluator:

- Should search for vulnerabilities in suitable vulnerability databases in all identifiable TOE/product components, and third party components.
- should report which search words/phrases were used (including the components above),
- shall report the vulnerability databases that were searched,
- should present the criteria used for dismissing irrelevant search results,
- should present a shortlist of possibly relevant vulnerabilities, and
- should investigate whether vulnerabilities in the shortlist are applicable, either by analysis, or by penetration testing. When the developer provides input to this analysis, the evaluator shall verify that the information is reasonable.

Components outside TOE

Sometimes the TOE is only a subset of the product delivered to the customer, and sometimes the TOE depends on a specific version of another product. In those cases, components and products outside the scope of TOE may have to be considered in the vulnerability assessment.

- When the delivery to the end user contains non-TOE components that are not trivial for the end user to replace at will, or that should not be changed, these components should be considered in the vulnerability assessment. In particular, public vulnerability databases should be searched for vulnerabilities applicable to the specific versions of these components.
- When the TOE depends on a specific version of an external IT product in the environment, this product should be considered in the vulnerability assessment. In particular, public vulnerability databases should be searched for vulnerabilities applicable to the specified version of the product.

Validity time for AVA

When the evaluation is completed, it is important that the vulnerability assessment was done recently. This reduce the likelihood that new vulnerabilities are discovered before certification.

- If 30 days has passed between the vulnerability assessment and the final version of the final evaluation report (FER), a new search for vulnerabilities in public vulnerability databases should be made and all new applicable vulnerabilities found should be considered. This may be documented separately, or in the AVA report.
- If a new applicable vulnerability is discovered before the TOE certification decision CSEC may

request the evaluator to consider this in the AVA report or in a separate AVA assessment update.

Reporting residual vulnerabilities

In CC, the evaluator is not expected to test for or determine the exploitability of potential vulnerabilities beyond those for which the perceived attack potential level is required to effect an attack. Any potential vulnerabilities judged to be beyond the perceived attack level required are classified as residual vulnerabilities. The procedure for vulnerability assessment in CC tends to disregard attacks which clearly cannot be performed (because they belong to a category two or more steps higher) at the attack potential perceived in the AVA_VAN component.

Since vulnerabilities requiring very high attack potential will typically not be recognized as potential vulnerabilities in the first place, only residual vulnerabilities corresponding to the next higher category of attack potential need to be reported. For example, the vulnerability assessment in AVA_VAN.2 assures resistance against attackers with an attack potential of Basic, and would not consider attacks that would require a Moderate or higher attack potential, and therefore an evaluator only needs to report residual vulnerabilities with a needed minimum attack potential of Enhanced-Basic in an AVA_VAN.2 evaluation. The attack potential categories are defined in the CEM, Appendix B: Basic, Enhanced-Basic, Moderate, High, and Beyond High.

Appended Documents