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

Scheme Note

Decision Date	Matter ID	
2017-11-30	CR-2354, CR-2470, CR-2589	
Decision by (Name/Title)	Scheme Note Number	Dnr
Mats Engquist, delegated by Dag Ströman, Head of CSEC	22	17FMV9859-1:1
Presentation by	Present at the Meeting	
Jerry Johanssson	CCB 2017-11-30	

Schematolkningens innebörd/Scheme Note Statement

Description and References

Background

This Scheme note relates to two issues regarding vulnerability assessment.

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 the certifier discovers a new applicable vulnerability before the TOE certification, and informs the evaluator, the evaluator should consider these in the AVA report or in a separate AVA assessment update.

Appended Documents