Network Device Interpretation # 202002

Clarification on developer disclosure of software components as part of AVA_VAN

Status: ☒ *Active* □ *Inactive*

Date: *4-Aug-2020*

End of proposed Transition Period (to be updated after TR2TD process): *4-Sep-2020*

Type of Change: □ Immediate application ☒ Minor change □ Major change

Type of Document: ☒ *Technical Decision* □ *Technical Recommendation*

Approved by: ☒ *Network iTC Interpretations Team* ☒ *Network iTC*

Affected Document(s): *ND SDv2.1, ND SDv2.2*

Affected Section(s): *AVA_VAN.1*

Superseded Interpretation(s): *None*

Issue:

ND SDv2.1 includes the following assurance activity related to the vulnerability analysis (AVA_VAN):

672 The developer shall provide documentation identifying the list of software and hardware components that compose the TOE. Hardware components should identify at a minimum the processors used by the TOE. Software components include applications, the operating system and other major components that are independently identifiable and reusable (outside the TOE) such as a web server and protocol or cryptographic libraries. This additional documentation is merely a list of the name and version number of the components, and will be used by the evaluators in formulating hypotheses during their analysis.

Please clarify if "*other major components that are independently identifiable and reusable*" must include the complete list of Linux third-party modules or is it limited to "*a web server and protocol or cryptographic libraries"* as specified in the "*such as*" list? Please also specify the expected outcome of the evaluation activity if a third-party module is discovered to be past EOL (end of life), abandonware, or impacted by unmitigated publicly disclosed vulnerability (e.g. CVE).

Resolution:

To address the issue raised in the issue section, the following changes shall be performed to the third paragraph of chapter 5.6.1.1 Evaluation Activity (Documentation) in ND SDv2.1/2.2 (i.e. para 672 in ND SDv2.1; para 674 in ND SDv2.2):

<old>

The developer shall provide documentation identifying the list of software and hardware components that compose the TOE. Hardware components should identify at a minimum the processors used by the TOE. Software components include applications, the operating system and other major components that are independently identifiable and reusable (outside the TOE) such as a web server and protocol or cryptographic libraries. This additional documentation is merely a list of the name and version number of the components, and will be used by the evaluators in formulating hypotheses during their analysis. *</old>*

shall be replaced by

<new>

The developer shall provide documentation identifying the list of software and hardware components that compose the TOE. Hardware components should identify at a minimum the processors used by the TOE. Software components include applications, the operating system and other major components that are independently identifiable and reusable (outside of the TOE), for example a web server, protocol or cryptographic libraries**, (independently identifiable and reusable components are not limited to the list provided in the example)**. This additional documentation is merely a list of the name and version number of the components and will be used by the evaluators in formulating **vulnerability** hypotheses during their analysis.

</new>

Rationale:

Provided in the Resolution section.

Further clarification: NDcPP does not make a distinction between developer created components and third-party components in the context of vulnerabilities. Therefore, neither the source of the component (e.g. vendor-developed vs. third-party), nor its current phase in the component life-cycle (e.g. end-of-life) have any bearing on the assessment of whether the component (and therefore the combined TOE) are vulnerable. Furthermore, the TOE developer assumes the responsibility to address and mitigate the impact of unmitigated/unpatched publicly disclosed vulnerabilities in third-party components used within the TOE in order to achieve certification.

Further Action:

None

Action by Network iTC:

None