Network Device Interpretation # 202015

Vulnerability Analysis Search Criteria

Status: ☒ *Active* ☐ *Inactive*

Date: *29-Sep-2020*

End of proposed Transition Period (to be updated after TR2TD process): *29-Oct-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): *NDSDv2.2*

Affected Section(s): *AVA_VAN.1*

Superseded Interpretation(s): *None*

Issue:

Supporting Document A. Vulnerability Analysis includes the following text:

"The search criteria to be used when searching the sources published after the publication date of the cPP shall include:

• The terms "router" and "switch" (or similar generic term describing the device type of the TOE)

• The following protocols: TCP"

Considering that "shall" is used, must the search criteria always utilize these exact search terms regardless of TOE technology type and protocols used?

*Also when stating: "*The search criteria to be used when searching the sources published after the publication date of the cPP*" does this mean that search criteria matches published before the cPP publication date can be discarded as irrelevant?*

Resolution:

The NIT acknowledges the issue described in the 'Issue' section above. Therefore, *NDSDv.2.2* paragraph 682 in section A.1.1 Type 1 Hypotheses - Public-Vulnerability-Based shall be replaced as follows:

<old>
"The search criteria to be used when searching the sources published after the publication date of the cPP shall include:

- The terms “router” and “switch” (or similar generic term describing the device type of the TOE)
- The following protocols: TCP
- Any protocols not listed above supported (through an SFR) by the TOE (these will include at least one of the remote management protocols (IPsec, TLS, SSH))
- The TOE name (including appropriate model information as appropriate)

</old>

shall be replaced by

<new>
According to section 5.6.1.1, the developer shall provide documentation identifying the list of software and hardware components that compose the TOE. The evaluator shall independently verify this list for completeness by comparing it to the security functionality defined in the TSS of the ST and ensuring that all expected components are accounted for.

Hardware components should identify at a minimum the processors used by the TOE. Software components that are in the scope of this requirement include libraries, frameworks, operating system and other major components that are independently identifiable and reusable (i.e. can be present in other products) components. The evaluator shall use the components list and determine that the TOE and its components are free of unmitigated vulnerabilities. It is expected that all remotely exploitable vulnerabilities present in the network device shall be considered as part of vulnerability assessment ("network device" is used to refer to the entire device and is not limited to the claimed security functionality).

The search criteria to be used when searching the sources shall include:

- The list of software and hardware components that compose the TOE
- The TOE name (including model information as appropriate)

As the search terms can contain proprietary information and there is a possibility that this information could be used by attackers to identify potential attack surfaces, there is no expectation that search terms containing proprietary information are published in any public-facing document.
</new>

In addition, *NDSDv.2.2* paragraph 681 in section A.1.1 Type 1 Hypotheses - Public-Vulnerability-Based shall be replaced as follows:

<old>
The evaluators shall perform a search on the sources listed in Section A.4 to determine a list of potential flaw hypotheses that are more recent that the publication date of the cPP, and those that are specific to the TOE and its components as specified by the additional documentation mentioned above. Any duplicates – either in a specific entry, or in the flaw hypothesis that is generated from an entry from the same or a different source – can be noted and removed from consideration by the evaluation team.
</old>

shall be replaced by

<new>
The evaluators shall perform a search on the sources listed in Section A.4 to determine a list of potential flaw hypotheses that are specific to the TOE and its components as specified by the additional documentation mentioned above. Any duplicates – either in a specific entry, or in the flaw hypothesis that is generated from an entry from the same or a different source – can be noted and removed from consideration by the evaluation team.
</new>

Rationale:

The original wording was misleading as it could be misread as requirement to limit the vulnerability search to the exact search terms and timeframes as provided as example in the paragraph. The updated wording clarifies the scope of the expected effort.

Further Action:

None

Action by Network iTC:

None