

Network Device Interpretation # 201926

FTP_ITC.1 with signed downloads

Status: Active Inactive

Date: 17-Dec-2019

End of proposed Transition Period (to be updated after TR2TD process): 17-Dec-2019

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): NDcPPv2.1

Affected Section(s): FTP_ITC.1

Superseded Interpretation(s): None

Issue:

A customer has a network device that supports the download of digitally signed firmware updates over a HTTP connection. (HTTPS is not supported for these downloads.) The signed image is validated prior to the installation of the update.

From NIAP's perspective, is this connection compliant with the FTP_ITC.1 requirement?

Rationale:

NDcPP v2.1 FTP_ITC.1 states the TSF shall be capable of using [selection: IPsec, SSH, TLS, DTLS, HTTPS] to provide a trusted communications channel between itself and authorized IT entities ...

There's no definition in the cPP of "authorized IT entities", but it would seem that the download site URL would implicitly refer to an "authorized IT entity" simply by the admin authorizing the download from the URL. Thus, one could argue that this HTTP-only download connection is non-compliant with NDcPP v2.1's FTP_ITC.1.

Resolution:

NDcPP requires exact conformance and HTTP is not among the options provided in the selection for FTP_ITC.1. An HTTP connection is therefore not conformant with the FTP_ITC.1 requirements. For the use case of downloading signed firmware updates, NDcPP doesn't mandate the use of a trusted channel according to FTP_ITC.1. For details please see the resolution for RfI#(2016)57rev2.

Rationale:

Provided in the Resolution section.

Further Action:

None

Action by Network iTC:

None