Network Device Interpretation # 201719

Support for X509 ssh rsa authentication IAW RFC 6187

Status: ☒ *Active* ☐ *Inactive*

Date: *25-Sep-2017*

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

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

Affected Document(s): *NDcPP V2.0*

Affected Section(s): FCS_SSHC_EXT.1.5/FCS_SSHS_EXT.1.5

Superseded Interpretation(s): *None.*

Issue:

Issue:

RFC 6187 is listed as a selectable option (in FCS_SSH*_EXT.1.1) for SSH conformance however there are no options (in FCS_SSH*_EXT.1.5) for X509v3 authentication for SSH RSA public-key based authentication that presents inconsistencies and operational constraints.

Proposed Resolution:

In NDcPP v2.0 change FCS_SSHC_EXT.1.5/FCS_SSHS_EXT.1.5 as follows, to add x509v3-ssh-rsa and x509v3-rsa2048-sha256 as selections:

FCS_SSHC_EXT.1.5/FCS_SSHS_EXT.1.5 The TSF shall ensure that the SSH public-key based authentication implementation uses [selection: ssh-rsa, ecdsa-sha2-nistp256, x509v3-ssh-rsa] and [selection: ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, x509v3-ecdsa-sha2-nistp256, x509v3-ecdsa-sha2-nistp384, x509v3-ecdsa-sha2-nistp521, x509v3-rsa2048-sha256, no other public key algorithms] as its public key algorithm(s) and rejects all other public key algorithms.

Rationale:

RFC 6187 includes ECDSA and RSA options. The NDcPPv2.0 has allowances for public-key based authentication for x509v3-ecdsa-sha2-nistp256, x509v3-ecdsa-sha2-nistp384, x509v3-ecdsa-sha2-nistp521, though none for support of x509v3-ssh-rsa or x509v3-rsa2048-sha256. This is inconsistent with the RFC.

Vendors cannot meet this requirement as written if their RFC-compliant x509v3 implementation of SSH only supports RSA and not ECDSA. Also without RSA support, we are placing operational constraints on customers by forcing an ECDSA PKI infrastructure for SSH when they may have an

RSA PKI infrastructure already in place for their TLS and/or IPsec solution, which is acceptable in the cPP.

Additionally, all of the other protocols in the cPP support RSA, and this leaves the SSH protocol without RSA certificate authentication. This omission is contrary to RFC 6187 in FCS_SSHC_EXT.1.5/FCS_SSHS_EXT.1.5 and the overall cryptographic requirements in the cPP.

References:

Refer RFC 6187 https://tools.ietf.org/rfcmarkup?doc=6187#section-3.2

Resolution:

The NIT acknowledges the issue described in the 'Issue' section above. In addition to adding x509v3-ssh-rsa and x509v3-rsa2048-sha256 to FCS_SSHC_EXT.1.5 and FCS_SSHS_EXT.1.5 the NIT proposes to merge the two selections. FCS_SSHC_EXT.1.5 and FCS_SSHS_EXT.1.5 shall therefore be modified as follows:

"FCS_SSHC_EXT.1.5/FCS_SSHS_EXT.1.5 The TSF shall ensure that the SSH public-key based authentication implementation uses [selection: ssh-rsa, ecdsa-sha2-nistp256, x509v3-ssh-rsa, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, x509v3-ecdsa-sha2-nistp256, x509v3-ecdsa-sha2-nistp384, x509v3-ecdsa-sha2-nistp521, x509v3-rsa2048-sha256] as its public key algorithm(s) and rejects all other public key algorithms."

The application note for FCS_SSHC_EXT.1.5 shall be modified as follows:

"If x509v3-ssh-rsa, x509v3-ecdsa-sha2-nistp256, x509v3-ecdsa-sha2-nistp384, x509v3-ecdsa-sha2-nistp521 or x509v3-rsa2048-sha256 are selected, then the list of trusted certification authorities must be selected in FCS_SSHC_EXT.1.9 and the FIA_X509_EXT SFRs in Appendix B are applicable.

It is recommended to configure the TOE to reject presented RSA keys with a key length below 2048 bit."

The application note for FCS_SSHS_EXT.1.5 shall be modified as follows:

"If x509v3-ssh-rsa, x509v3-ecdsa-sha2-nistp256, x509v3-ecdsa-sha2-nistp384, x509v3-ecdsa-sha2-nistp521 or x509v3-rsa2048-sha256 are selected, then the FIA_X509_EXT SFRs in Appendix B are applicable.

It is recommended to configure the TOE to reject presented RSA keys with a key length below 2048 bit."

The application note for FCS_SSHC_EXT.1.9 shall be modified as follows:

"The list of trusted certification authorities can only be selected if x509v3-ssh-rsa, x509v3-ecdsa-sha2-nistp256, x509v3-ecdsa-sha2-nistp384, x509v3-ecdsa-sha2-nistp521 or x509v3-rsa2048-sha256 are selected in FCS_SSHC_EXT.1.5."

Rationale:

As provided in the 'Issue' section.

Note: The NIT usually does not cover RfIs related to additional cryptographic algorithms or cipher suites. Adding the ciphers for X509v3 authentication for SSH RSA public-key based authentication has already been discussed and accepted by the editorial team for NDcPP V2.0. Unfortunately, it has been overlooked to integrate it in the drafting process for the final version of NDcPP V2.0. Therefore the NIT has agreed to resolve this issue through an RfI.

Further Action:

None

Action by Network iTC:

None