Network Device Interpretation # 202014

Additional test for CVE-2020-0601

Status: ☒ *Active* □ *Inactive*

Date: *4-Aug-2020*

End of proposed Transition Period (to be updated after TR2TD process): *4-Aug-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): *FIA_X509_EXT.1/REV, FIA_X509_EXT.1/ITT*

Superseded Interpretation(s): *None*

Issue:

Validation of certificates, if not done correctly, can introduce vulnerabilities (like CVE-2020-0601). Testing to ensure proper validation of Elliptic Curve Cryptography (ECC) certificates is lacking allowing spoofing attacks to exist in evaluated products.

Resolution:

The issue identified in the 'Issue' section is acknowledged. Therefore, the following test shall be added to the tests for FIA_X509_EXT.1/REV and FIA_X509_EXT.1/ITT

<new>

"Test 8: [Conditional] If EC certificates are supported as indicated in FCS_COP.1/SigGen, the evaluator shall establish a valid, trusted certificate chain consisting of an EC leaf certificate, an EC Intermediate CA certificate not designated as a trust anchor, and an EC certificate designated as a trusted anchor, where the elliptic curve parameters are specified as a named curve. The evaluator shall confirm that the TOE validates the certificate chain. The evaluator shall replace the intermediate certificate in the certificate chain for Test 8 with a modified certificate, where the modified intermediate CA has a public key information field where the EC parameters uses an explicit format version of the Elliptic Curve parameters in the public key information field of the intermediate CA certificate from Test 8, and the modified Intermediate CA certificate is signed by the trusted EC root CA, but having no other changes. The evaluator shall confirm the TOE treats the certificate as invalid. "

</new>

Rationale:

The new (conditional) test will help prevent exploitation of spoofing vulnerabilities. Note, that this resolution matches the already published NIAP TD0527.

For background information about the test specified above, see RFC5480, section 2.1.1.

Further Action:

None

Action by Network iTC:

None