Network Device Interpretation # 201818

local vs. remote administrator accounts

Status: ☒ *Active* ☐ *Inactive*

Date: *6-Mar-2019*

End of proposed Transition Period (to be updated after TR2TD process): *6-Jun-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): *NDcPP V2.0e, NDcPP V2.1, FWcPP V2.0e*

Affected Section(s): *FIA_AFL.1, FIA_UAU_EXT.2*

Superseded Interpretation(s): *None*

Issue:

Issue:

FIA_AFL.1 is causing issues for network device vendors that don't logically distinguish between local and remote administrative consoles.

In NDcPPv1.0, the local console was just a location statement. In NDcPPv2.0, FIA_AFL.1 forces the local console to function differently from the remote consoles.

For a network device that doesn't distinguish between local and remote administrators (i.e., no local console, only an Ethernet port/connector that is used by both local and remote administrators), can the FIA_AFL.1 requirement be satisfied by having one administrative account that does not lock after a defined number of failed login attempts and all the remaining administrative accounts that do lock as alluded to in Application Note 16?

Application Note 16 states:

"This could be addressed by (for example) requiring a separate account for local Administrators or …".

In this case, the non-locking administrative account would be logically called the "local Administrator account" in the ST, but the only difference between it and the other administrative accounts would be that it would not lock. This would basically leave this one non-locking account vulnerable to unmitigated password attacks on the network used by the remote administrators.

Proposed Resolution:

If this approach is sufficient or insufficient to meet NDcPP v2.0, please provide more clarification on what is expected.

Resolution:

The NIT acknowledges that network devices that do not distinguish between local and remote administrative access are common and that meeting the FIA_AFL requirements to prevent complete administrative lockout outlined in the Application Note 16 (NDcPPv2.0e)/17 (NDcPPv2.1) could be problematic when FIA_AFL requirement applied to individual accounts instead of authentication methods; however, the NIT may only provide interpretations on the requirements.

Additionally, the NIT does not believe that any requirement in the cPP mandates a specific hardware implementation (e.g. RS-232 management port) and therefore a distinction between local and remote administrative access is essentially logical. However, such distinction cannot be purely label-based as outlined in the issue section of this RFI and must have functional components associated with it.

The NIT agreed on the following working definition of local administrative access (or local session) and relaxation of account unlocking requirements:

The first three sentences of NDcPPv2.1 FMT_SMF.1 Application Note 23(NDcPPv2.0e)/24(NDcPPv2.1) shall be updated as follows:

The TOE must provide functionality for both local and remote administration in general. This cPP does not mandate, though, a specific security management function to be available either through the local administration interface, the remote administration interface or both. Local administration is defined as administration using a dedicated physical interface that (from the TOE's point of view) is directly connected to the device(s) the administrator interacts with and therefore falls under the physical protection (OE.PHYSICAL). Any administrator choice to extend a local console so it is remotely accessible (e.g. console server) is outside the scope of the NDcPP. The following are examples of compliant local administrative interfaces:

a. RS-232 terminal.
b. Peripherals (e.g. keyboard, monitor, mouse).
c. Use of a dedicated Ethernet port that only supports communication with a whitelisted local IP address. Guidance shall provide instructions for configuring the whitelisted IP address as well as ensuring physical protection from the TOE to the IP address. The management protocol does not need to meet FTP_TRP.1/Admin; however, the appropriate authentication must be claimed in FIA_UAU_EXT.2. Note: A local management protocol that does not meet FTP_TRP.1/Admin shall not be available on any other network ports.

NDcPPv2.0e/2.1 Supporting Document, FMT_SMF.1, Section 2.4.4.1 shall be appended as follows:

The evaluator shall examine the TSS and Guidance Documentation to verify they both describe the local administrative interface. The evaluator shall ensure the Guidance Documentation includes appropriate warnings for the administrator to ensure the interface is local.

NDcPPv2.0e/2.1 FIA_UAU_EXT.2 SFR shall be modified as follows:

FIA_UAU_EXT.2.1 The TSF shall provide a local [selection: *password-based, SSH public key-based, certificate-based, [assignment: other authentication mechanism(s)]*] authentication mechanism to perform local administrative user authentication.

NDcPPv2.0e/2.1 FIA_UAU_EXT.2 Application Note 19(NDcPPv2.0e)/20(NDcPPv2.1) shall be appended as follows:

SSH public key-based and certificate-based authentication mechanisms can only be selected when an appropriate cryptographic protocol is used to provide local administrative access.

NDcPPv2.0e/2.1 FIA_AFL.1 SFRs shall be updated as follows:

FIA_AFL.1.1 The TSF shall detect when an Administrator configurable positive integer within [assignment: range of acceptable values] unsuccessful authentication attempts occur related to *Administrators attempting to authenticate remotely using a password*.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met, the TSF shall [selection: *prevent the offending Administrator from successfully establishing remote session using any authentication method that involves a password until [assignment: action to unlock] is taken by an Administrator; prevent the offending Administrator from successfully establishing remote session using any authentication method that involves a password until an Administrator defined time period has elapsed*].

NDcPPv2.0e/2.1 FIA_AFL.1 Application Note 16(NDcPPv2.0e)/17(NDcPPv2.1) first sentence shall be replaced as follows:

<old>This requirement applies to a defined number of successive unsuccessful authentication attempts and does not apply to an Administrator at the local console, since it does not make sense to lock a local Administrator's account in this fashion.</old>

Shall be replaced by

<new>This requirement applies to a defined number of successive unsuccessful remote password-based authentication attempts and does not apply to local Administrative access, since it does not make sense to lock a local Administrator's account in this fashion. Compliant TOEs may optionally include cryptographic authentication failures and/or local authentication failures in the number of unsuccessful authentication attempts.</new>

Rationale:

As stated in the resolution section.

Further Action:

None.

Action by Network iTC:

None.