Network Device Interpretation # 5

Using /dev/random as third party source of entropy

Status: ☒ *Active* ☐ *Inactive*

Date: *22-Feb-2016*

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

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

Affected Document(s): *NDcPP V1.0, FWcPP V1.0*

Affected Section(s): *FCS_RBG_EXT.1.2*

Superseded Interpretation(s): *None.*

Issue:

Can /dev/random be considered a third party source of entropy? While a vendor should have access to the code and be able to analyze the raw entropy, it is likely that the vendor will not have written any part of /dev/random and will not have insight into how it works. While we understand there can be significant variations in /dev/random from one platform to another, the average developer will not know what to look for or be able to provide meaningful analysis without detailed guidance.

Resolution:

NIT fully supports the response provided by NIAP on that request.

"No, this is not considered a third party entropy source. There is substantial public documentation regarding /dev/random and it is expected that a vendor understand the source they are using to provide the basic security of their device."

Rationale:

N/A

Further Action:

None.

Action by Network iTC:

None.