PANDUIT® infrastructure for a connected world

Panduit Data Center; Power, Environmental and Access Control Product Statement

Spectre and Meltdown Vulnerabilities - (CVE-2017-5715, CVE-2017-5753, CVE-2017-5754)

Products:

EPA126 / (Eagle-i)	Gateway
EPA064 / (Hawk-i3	Gateway
EP042 / (RackMS)	Gateway
E24 / (EnviroHawk-2)	Gateway
NE-PDU	G3 Network Attached Power Strip

The above listed Gateway and G3 Network Power Strip products use an ARM based microprocessor. The microprocessor manufacturer has made a security statement regarding this processor (which may be viewed on Digi Inc. Web site: https://www.digi.com/resources/security.)

Panduit is aware of the **Spectre** and **Meltdown** vulnerabilities that were recently announced. These vulnerabilities impact the confidentiality of data running on Intel, AMD and ARM processors.

For the Panduit hardware products listed above, we do not use Intel or AMD processors, and therefore the "**Meltdown**" vulnerability does not affect these Panduit hardware products.

For the **Spectre** vulnerability, the listed Panduit products only support the execution of its own embedded firmware, there is no support for uploading 3rd party applications, and there is no support for executing 3rd party applications either on the gateways, G3 PDUs or their attached peripherals (GW-PDUs, Sensors etc.) and therefore these products are not directly affected by the **Spectre** vulnerability.

For more information on these vulnerabilities, please see the website https://meltdownattack.com/

Panduit Data Center
Product Engineering Group
2018 Jan

Ref RD02173