

9 January 2018
300382478 / pbsa56

Security Advisory for FL SWITCH 3xxx, FL SWITCH 4xxx, FL SWITCH 48xx products [CVE-2017-16741]

Synopsis

CVE-2017-16741: Ability to see switch information using Monitor Mode.

Affected products

All Phoenix Contact managed FL SWITCH 3xxx, 4xxx, 48xx products running firmware version 1.0 to 1.32

Issue

Any user that has network access to a Phoenix Contact managed FL SWITCH device may read diagnostic information from the device's Web interface.

Details

By default, Monitor Mode provides read-only access to some of the managed FL SWITCH devices web pages. This includes information about the model, subnet mask, uptime, and utilization.

Mitigation

Customers using Phoenix Contact managed FL SWITCH devices with affected firmware versions are recommended to update to firmware version 1.33 or higher which fixes this vulnerability. The updated firmware may be downloaded from the managed switch product page on the Phoenix Contact website.