PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg, Germany
Telefon: +49 5235 300
Telefax: +49 5235 3-41200
Internet: http://www.phoenixcontact.com
USt-Id-Nr.: DE124613250
WEEE-Reg.-Nr.: DE50738265

PHOENIX CONTACT GmbH & Co. KG · 32825 Blomberg

11 May 2018
300405373/pbsa56

Security Advisory for FL SWITCH 3xxx, FL SWITCH 4xxx, FL SWITCH 48xx products [CVE-2018-10729]

Advisory Title

Insecure Direct Object Reference to Read-Only FL SWITCH Configuration File.

Advisory ID

CVE-2018-10729
VDE-2018-005

Vulnerability Description

Web interface CGI applications may copy the contents of the running configuration file to a commonly accessed file. Clever manipulation of a web login request can expose the contents of this file through to the web browser. A successful web interface login attempt is not required to read the configuration file contents.

Affected products

All Phoenix Contact managed FL SWITCH 3xxx, 4xxx, 48xx products running firmware version 1.0 to 1.33

Impact

FL SWITCH Configuration File can be read by unauthenticated user.
Classification of Vulnerability
Base Score: 5.3 (Medium)
Vector: CVSS: 3.0 /AV:N /AC:L /PR:N /UI:N /S:U /C:L /I:N /A:N

Temporary Fix / Mitigation

Customers using Phoenix Contact managed FL SWITCH devices with affected firmware versions are recommended to disable the switch Web Agent.

Remediation

Customers using Phoenix Contact managed FL SWITCH devices with affected firmware versions are recommended to update the firmware to version 1.34 or higher which fixes this vulnerability. The updated firmware may be downloaded from the managed switch product page on the Phoenix Contact website.

Acknowledgement

This vulnerability was discovered by Semen Sokolov (Positive Technologies).