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

15 January 2019
300405373/pbsa56

Security Advisories for FL SWITCH 3xxx, FL SWITCH 4xxx, FL SWITCH 48xx products

Contents

Denial-of-service attack to web pages (HTTP) (CWE-400, CWE-941) 2
Improper Restriction of Excessive Authentication Attempts (CWE-307) 3
Insecure Transmission of Sensitive Information (CWE-319, CWE-310) 4
Cross-site Request Forgery (CSRF) (CWE-352) 5
Vulnerability in the Switch Security Library 6
Insecure Storage of Sensitive Information (CWE-922) 7

Advisory Title

Denial-of-service attack to web pages (HTTP) (CWE-400, CWE-941)

Advisory ID

CVE-2018-13994
VDE-2019-001

Vulnerability Description

An attacker can initiate a web Denial of Service attack by producing more than 120 Web UI connections.

Affected products

All Phoenix Contact managed FL SWITCH 3xxx, 4xxx, 48xx products running firmware version 1.0 to 1.34

Impact

If vulnerability is exploited, the attacker may deny all web access to the switch, including current connections.

Classification of Vulnerability

Base Score: 7.5(High)
Vector: CVSS: 3.0 /AV:N /AC:L /PR:N /UI:N /S:U /C:N /I:N /A:H

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 1.35 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 Evgeniy Druzhinin, Georgy Zaytsev, and Ilya Karpov (Positive Technologies).

...

Advisory Title

Improper Restriction of Excessive Authentication Attempts (CWE-307)

Advisory ID

CVE-2018-13990
VDE-2019-001

Vulnerability Description

The switch needs an extended login time-out feature to prevent high-speed automated username and password combination guessing. An attacker may gain access by such a brute forcing of usernames and passwords.

Affected products

All Phoenix Contact managed FL SWITCH 3xxx, 4xxx, 48xx products running firmware version 1.0 to 1.34

Impact

If vulnerability is exploited, the attacker can gain access to the switch by brute forcing Web UI service passwords.

Classification of Vulnerability

Base Score: 8.6(High)
Vector: CVSS: 3.0 /AV:N /AC:L /PR:N /UI:N /S:U /C:H /I:L /A:L

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 1.35 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 Evgeniy Druzhinin and Ilya Karpov (Positive Technologies).

...

Advisory Title

Insecure Transmission of Sensitive Information (CWE-319, CWE-310)

Advisory ID

CVE-2018-13992
VDE-2019-001

Vulnerability Description

The default setting of the Web UI (HTTP) allows user credentials to be transmitted unencrypted.

Affected products

All Phoenix Contact managed FL SWITCH 3xxx, 4xxx, 48xx products running firmware version 1.0 to 1.34

Impact

If vulnerability is exploited, the user's credentials can be read by examining the Web UI login traffic between the switch and the user.

Classification of Vulnerability

Base Score: 8.2(High)
Vector: CVSS: 3.0 /AV:N /AC:L /PR:N /UI:N /S:U /C:H /I:L /A:N

Temporary Fix / Mitigation

Customers using Phoenix Contact managed FL SWITCH devices recommended to disable the switch Web Agent or enable Web encryption (HTTPS).

Remediation

Customers using Phoenix Contact managed FL SWITCH devices recommended to disable the switch Web Agent or enable Web encryption (HTTPS).

Acknowledgement

This vulnerability was discovered by Evgeniy Druzhinin and Ilya Karpov (Positive Technologies).

Advisory Title

Cross-site Request Forgery (CSRF) (CWE-352)

Advisory ID

CVE-2018-13993
VDE-2019-001

Vulnerability Description

Additional Cross-site Request Forgery (CSRF) protections are required to be implemented in the Web UI. This attack tricks may trick the web browser into transmitting unwanted commands.

Affected products

All Phoenix Contact managed FL SWITCH 3xxx, 4xxx, 48xx products running firmware version 1.0 to 1.34

Impact

If vulnerability is exploited, an attacker could persuade a user to follow a malicious Web UI link. This could allow the attacker to submit arbitrary requests to the affected software via the user's web browser with the user's privileges.

Classification of Vulnerability

Base Score: 8.8(High)
Vector: CVSS: 3.0 /AV:N /AC:L /PR:N /UI:R /S:U /C:H /I:H /A:H

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 1.35 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 Evgeniy Druzhinin and Ilya Karpov (Positive Technologies).

Advisory Title

Vulnerability in the Switch Security Library

Advisory ID

CVE-2017-3735
VDE-2019-001

Vulnerability Description

The existing switch security library is vulnerable to CVE-2017-3735 DoS.

Affected products

All Phoenix Contact managed FL SWITCH 3xxx, 4xxx, 48xx products running firmware version 1.0 to 1.34

Impact

When using Web HTTPS settings, it is possible to do an inaccurate read of the certificate, which could also result in an incorrect display of the certificate.

Classification of Vulnerability

Base Score: 5.3 MEDIUM
Vector: CVSS: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/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 1.35 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 Evgeniy Druzhinin and Ilya Karpov (Positive Technologies).

Advisory Title

Insecure Storage of Sensitive Information (CWE-922)

Advisory ID

CVE-2018-13991
VDE-2019-001

Vulnerability Description

An attacker may extract the switch's default private keys from its firmware image.

Affected products

All Phoenix Contact managed FL SWITCH 3xxx, 4xxx, 48xx products running firmware version 1.0 to 1.34

Impact

An attacker could perform man-in-the-middle attacks or deploy malicious but trusted web sites.

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 1.35 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 Evgeniy Druzhinin and Ilya Karpov (Positive Technologies).