PHOENIX CONTACT GmbH & Co. KG · 32825 Blomberg

2019-03-20
300436449/pbsa56

Security Advisory for Phoenix Contact FL NAT SMx

Advisory Title

Unauthorized user can get access to the WEB-UI of the device if an authorized IP is used

Advisory ID

CVE-2019-9744
VDE-2019-006

Vulnerability Description

After login the source IP is used as the session identifier, so that users sharing the same source IP are able to gain full authenticated access to the WEB-UI.

The access attempt will only be successful if the former authorized session has not been terminated by the authorized user or by session timeout.

Affected products

2702443	FL NAT SMN 8TX-M
2989352	FL NAT SMN 8TX-M-DMG
2989365	FL NAT SMN 8TX
2989378	FL NAT SMCS 8TX

Impact

If an unauthorizes user manages to get access as described above, he can gain full access to the device configuration.

Personally liable partner:
Phoenix Contact Verwaltungs GmbH
Amtsgericht Lemgo HRB 5273
Kom. Ges. Amtsgericht Lemgo HRA 3746

Executive Vice Presidents:
Frank Stührenberg (CEO)
Roland Bent
Prof. Dr. Gunther Olesch
Axel Wachholz

Deutsche Bank AG
(BLZ 360 700 50) 226 2665 00
BIC: DEUTDEDEXXX
IBAN:
DE93 3607 0050 0226 2665 00

Commerzbank AG
(BLZ 476 400 51) 226 0396 00
BIC: COBADEFFXXX
IBAN:
DE31 4764 0051 0226 0396 00

...

Classification of Vulnerability

Base Score: 8.8
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 FL NAT SMx devices are recommended to operate the devices in closed networks or protected with a suitable firewall.
For detailed information on our recommendations for measures to protect network-capable devices, please refer to our application note:

https://www.phoenixcontact.com/assets/downloads_ed/local_pc/web_dwl_technical_info/ah_en_industrial_security_107913_en_01.pdf

To protect the device from an attacker who has gained access to the closed network, or if there is a possibility that multiple users might share a VPN connection with a single endpoint IP, it might be considered to:

- log off from the WEB-UI immediately after administration
- disable the WEB-UI and use configuration access via SNMP instead.

Acknowledgement

This vulnerability was discovered by Maxim Rupp (rupp.it)