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

2020-05-18
300462358/pbsa56

Security Advisory for Phoenix Contact FL NAT 2xxx

Advisory Title

Users unauthorized by MAC based port security or 802.1x port security can get access to a routed subnet.

Advisory ID

CVE-2019-18352
VDE-2019-020

Vulnerability Description

If MAC-based port security or 802.1x port security is enabled, the FL NAT 2xxx will unintentionally grant access to unauthorized devices in case of routed transmission.

```
Subnet 2---(Ports belonging to subnet 2)
                  |
            FL NAT 2xxx
                  |
           (Ports belonging to subnet 1, port sec ON)---- 2nd device
                                                    |
                                                    -- unauthorized device
```

The unauthorized device can access other devices in subnet 2 but cannot access the 2nd device in subnet 1

Affected products

Article no.	Article	Affected Firmware	Current Firmware
2702882	FL NAT 2208	< 2.90	download
2702981	FL NAT 2304-2GC-2SFP	< 2.90	download

...

Impact

If port security is enabled on a port, a device not authorized by MAC based port security or 802.1x based port security can access another subnet via the FL NAT 2xxx device that is routing between the subnet the unauthorized device is residing in and the 2nd subnet.

Classification of Vulnerability

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

Temporary Fix / Mitigation

Users should take care that network security is not relying solely on separating subnets with MAC or 802.1x based port security if the FL NAT 2xxx device is serving as a router between the subnets.

Update 2020-05-18: Firmware V2.90 is released and available for download.

NOTE: If traps/logs/syslog for unauthorized access are enabled, notifications about the unauthorized access will be sent.

Acknowledgement

This vulnerability was discovered during internal audits due to a customer complaint.