

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

### **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](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)