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

20 March 2019
300436698 / pbsa56

Security Advisory for RAD-80211-XD and RAD80211-XD/HP-BUS [CVE-2019-9743]

Advisory Title

Command injection through WebHMI utility.

Advisory ID

CVE-2019-9743
VDE-2019-007

Vulnerability Description

A WebHMI utility may be exploited by any logged in user allowing the execution of arbitrary OS commands on the server. This provides the opportunity for a command injection attack.

Affected products

2885728	RAD-80211-XD
2900047	RAD-80211-XD/HP-BUS

Impact

If vulnerability is exploited, the attacker may execute system level commands at will with administrative privileges.

Classification of Vulnerability

Base Score: 9.9 (Critical)
Vector: CVSS: 3.0 /AV:N /AC:L /PR:L /UI:N /S:C /C:H /I:H /A:H

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

...

Temporary Fix / Mitigation

Customers using Phoenix Contact 802-11XD radio modules 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

Remediation

The product has been removed from active maintenance due to obsolescence. For this reason, it is recommended that concerned customers upgrade to the active FL WLAN product line.

Acknowledgement

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