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 November 2022
2022/00006

Security Advisory for FL MGUARD, TC MGUARD

Publication Date: 2022-11-15
Last Update: 2022-11-15
Current Version: V1.0

Advisory Title

Possible denial of service on HTTPS management interface

Advisory ID

CVE-2022-3480

VDE-2022-051

Vulnerability Description

A denial of service of the HTTPS management interface of FL MGUARD and TC MGUARD devices can be triggered by a larger number of unauthenticated HTTPS connections, incoming from different source IP's. Configuring firewall limits for incoming connections cannot prevent the issue.

Affected products

Article no	Article	Affected versions
2700642	FL MGUARD RS2000 TX/TX VPN	< 8.9.0
2701875	FL MGUARD RS2005 TX VPN	< 8.9.0
2903441	TC MGUARD RS2000 3G VPN	< 8.9.0

...

2700634	FL MGUARD RS4000 TX/TX	< 8.9.0
2200515	FL MGUARD RS4000 TX/TX VPN	< 8.9.0
2701876	FL MGUARD RS4004 TX/DTX	< 8.9.0
2701877	FL MGUARD RS4004 TX/DTX VPN	< 8.9.0
2903440	TC MGUARD RS4000 3G VPN	< 8.9.0
2702139	FL MGUARD RS2000 TX/TX-B	< 8.9.0
2702259	FL MGUARD RS4000 TX/TX-P	< 8.9.0
2702470	FL MGUARD RS4000 TX/TX-M	< 8.9.0
2701274	FL MGUARD PCI4000	< 8.9.0
2701275	FL MGUARD PCI4000 VPN	< 8.9.0
2701277	FL MGUARD PCIE4000	< 8.9.0
2701278	FL MGUARD PCIE4000 VPN	< 8.9.0
2700967	FL MGUARD DELTA TX/TX	< 8.9.0
2700968	FL MGUARD DELTA TX/TX VPN	< 8.9.0
2700640	FL MGUARD SMART2	< 8.9.0
2700639	FL MGUARD SMART2 VPN	< 8.9.0
2702884	FL MGUARD CORE TX	< 8.9.0
2702831	FL MGUARD CORE TX VPN	< 8.9.0
2903588	TC MGUARD RS2000 4G VPN	< 8.9.0
2903586	TC MGUARD RS4000 4G VPN	< 8.9.0
1010461	TC MGUARD RS4000 4G VZW VPN	< 8.9.0
1010462	TC MGUARD RS2000 4G VZW VPN	< 8.9.0
1010463	TC MGUARD RS4000 4G ATT VPN	< 8.9.0
1010464	TC MGUARD RS2000 4G ATT VPN	< 8.9.0
2700197	FL MGUARD GT/GT	< 8.9.0
2700198	FL MGUARD GT/GT VPN	< 8.9.0
2702547	FL MGUARD CENTERPORT	< 8.9.0
2702820	FL MGUARD CENTERPORT VPN-1000	< 8.9.0

Impact

During the attack, the HTTPS management interface is no more accessible for valid users. Additionally, there may be an impact on the performance of other services of the FL MGUARD or TC MGUARD device. An unexpected reboot of the device is possible.

Classification of Vulnerability

CVE-2022-3480
Base Score: 7.5
Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CWE: CWE-770

CVE score and vector may have changed since publication of this advisory. You can find the current rating of a CVE at the respective link to the NVD website provided above.

...

Temporary Fix / Mitigation

Don’t allow access to the HTTPS management interface from untrusted networks.
In the default configuration, the access is only allowed from internal interfaces.

Remediation

The vulnerability is fixed in firmware version 8.9.0. We strongly recommend all affected users to upgrade to this or a later version.

Acknowledgement

This vulnerability was discovered by Alpha Strike Labs GmbH, Berlin.

We kindly appreciate the coordinated disclosure of this vulnerability by the finder.

PHOENIX CONTACT thanks CERT@VDE for the coordination and support with this publication.

History

V1.0 (2022-11-15): Initial publication