Security Advisory

Vulnerability in routers FL MGUARD and TC MGUARD

1 Advisory Information

Advisory ID: BOSCH-SA-931197

CVE Numbers and CVSS v3.1 Scores:

- CVE-2022-3480
  - Base Score: 7.5 (High)

Published: 03 Mar 2023

Last Updated: 03 Mar 2023

2 Summary

Possible denial of service on HTTPS management interface

The FL MGUARD and TC MGUARD devices sold by Bosch Rexroth are devices from Phoenix Contact that have been introduced as trade goods. A security advisory has been published by the manufacturer, which indicates that a denial of service of the HTTPS management interface of that devices can be triggered by a larger number of unauthenticated HTTPS connections, incoming from different source IP's [1]. Configuring firewall limits for incoming connections cannot prevent the issue.

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.

3 Affected Products

Parts No.	Parts Shorttext	PxC No.	Article
R901351745	FL MGUARD RS4000 TX/&	2700634	FL MGUARD RS4000 TX/TX
R901352542	FL MGUARD RS4000 VPN&	2200515	FL MGUARD RS4000 TX/TX VPN
R901541498	TC MGUARD RS4000 4G &	2903586	TC MGUARD RS4000 4G VPN
R911173814	FL MGUARD RS4000 TX/&	2200515	FL MGUARD RS4000 TX/TX VPN
R911173815	TC MGUARD RS2000 3G &	2903441	TC MGUARD RS2000 3G VPN
R911173816	TC MGUARD RS4000 3G &	2903440	TC MGUARD RS4000 3G VPN
R911173817	FL MGUARD DELTA TX/T&	2700967	FL MGUARD DELTA TX/TX
R911173818	FL MGUARD SMART2 VPN&	2700639	FL MGUARD SMART2 VPN
R913050362	FL MGUARD RS4004 TX/&	2701876	FL MGUARD RS4004 TX/DTX
R913051602	FL MGUARD RS4004 TX/&	2701877	FL MGUARD RS4004 TX/DTX VPN
R913056204	FL MGUARD RS2000 TX/&	2702139	FL MGUARD RS2000 TX/TX-B
R913058931	FL MGUARD RS2000 TX/&	2700642	FL MGUARD RS2000 TX/TX VPN
R913066122	TC MGUARD RS2000 4G &	2903588	TC MGUARD RS2000 4G VPN
R913076699	FL MGUARD RS4000 TX/&	2700634	FL MGUARD RS4000 TX/TX

Affected versions <= 8.9.0. Fixed version is available in the Security Advisory of the supplier [1].

4 Solution

4.1 Update to the latest released version

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

4.2 Temporary Fix / Mitigation

Don’t allow access to the HTTPS management interface from untrusted networks.

5 Vulnerability Details

5.1 CVE-2022-3480

CVE description: A remote, unauthenticated attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger number of unauthenticated HTTPS connections originating from different source IP’s. Configuring firewall limits for incoming connections cannot prevent the issue.

- Problem Type:
  - CWE-770 Allocation of Resources Without Limits or Throttling
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
  - Base Score: 7.5 (High)

6 Additional Resources

[1] Security Advisory for FL MGUARD, TC MGUARD:
https://dam-mdc.phoenixcontact.com/asset/156443151564/632a4cc10e4af34cb7b75da31a2f03a1/Security_Advisory_CVE-2022-3480.pdf

[2] Bosch Rexroth Security Guideline Electric Drives and Controls:
https://www.boschrexroth.com/various/utilities/mediadirectory/download/index.jsp?object_nr=R911342562

7 Revision History

03 Mar 2023: Initial Publication