Security Advisory
Vulnerability in routers FL MGUARD and TC MGUARD

1 Advisory Information

Advisory ID: BOSCH-SA-833074
CVE Numbers and CVSS v3.1 Scores:

- CVE-2022-4304
  - Base Score: 5.9 (Medium)
- CVE-2023-2673
  - Base Score: 5.8 (Medium)

Published: 04 Jul 2023
Last Updated: 04 Jul 2023

2 Summary

The FL MGUARD family 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 the devices are affected by two vulnerabilities regarding RSA decryption and MAC filtering [1].

3 Affected Products

Parts No.	Parts Shorttext	PxC No.	Article
R901351745	FL MGUARD RS4000 TX/&	2700634	FL MGUARD RS4000 TX/TX
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

4 Solution

4.1 Update to the latest released versions

The vulnerabilities are fixed in firmware version 8.9.1. We strongly recommend all affected users to upgrade to this or a later version. Please find further details on the security advisory of the supplier [1].

4.2 Compensatory measures

Compensatory measures are recommended which mitigate the risk. Always define such compensatory measures individually, in the context of the operational environment. Some measures are described in the "Security Guideline Electric Drives and Controls" [2], for example the network segmentation. In general, it is mandatory to implement the measures described in the "Security Guideline Electric Drives and Controls".

5 Vulnerability Details

5.1 CVE-2022-4304

CVE description: A timing based side channel exists in the OpenSSL RSA Decryption implementation which could be sufficient to recover a plaintext across a network in a Bleichenbacher style attack. To achieve a successful decryption an attacker would have to be able to send a very large number of trial messages for decryption. The vulnerability affects all RSA padding modes: PKCS#1 v1.5, RSA-OEAP and RSASVE.

For example, in a TLS connection, RSA is commonly used by a client to send an encrypted pre-master secret to the server. An attacker that had observed a genuine connection between a client and a server could use this flaw to send trial messages to the server and record the time taken to process them. After a sufficiently large number of messages the attacker could recover the pre-master secret used for the original connection and thus be able to decrypt the application data sent over that connection.

- Problem Type:
  - NVD-CWE-OTHER
- CVSS Vector String: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N
  - Base Score: 5.9 (Medium)

5.2 CVE-2023-2673

CVE description: Improper Input Validation vulnerability in PHOENIX CONTACT FL/TC MGUARD Family in multiple versions may allow UDP packets to bypass the filter rules and access the solely connected device behind the MGUARD which can be used for flooding attacks.

- Problem Type:
  - CWE-20 Improper Input Validation
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:L
  - Base Score: 5.8 (Medium)

6 Additional Resources

[1] Security Advisory for the FL MGUARD family of devices:
https://dam-mdc.phoenixcontact.com/asset/156443151564/6d4cfd9c39df5147a93b66411432b990/Security_Advisory-CVE-2022-4304_CVE-2023-2673.pdf

[2] Security Guideline Electric Drives and Controls:
https://www.boschrexroth.com/de/de/myrexroth/media-directory-download?object_nr=R911342562

7 Revision History

04 Jul 2023: Initial Publication