Security Advisory

Vulnerability in routers FL MGUARD and TC MGUARD

1 Advisory Information

Advisory ID: BOSCH-SA-982696

CVE Numbers and CVSS v3.1 Scores:

- CVE-2022-0778
  - Base Score: 7.5 (High)

Published: 27 Apr 2022

Last Updated: 27 Apr 2022

2 Summary

The FL MGUARD and TC MGUARD safety 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 devices are affected by a possible infinite loop within an OpenSSL library method [1].

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
R913073676	FL MGUARD RS4000 TX/&	1053403	FL MGUARD RS4000 TX/TX VPN/K1
R913073677	FL MGUARD SMART2 VPN&	1053405	FL MGUARD SMART2 VPN/K1
R913076699	FL MGUARD RS4000 TX/&	2700634	FL MGUARD RS4000 TX/TX

Affected versions <= 8.8.5. Fixed version is available in the Security Advisory of the supplier [1].

4 Solution

4.1 Update to the latest released versions

It is strongly recommended to update the firmware version of the affected devices. Please find further details on the security advisory of the supplier [1].

5 Vulnerability Details

5.1 CVE-2022-0778

CVE description: The BN_mod_sqrt() function, which computes a modular square root, contains a bug that can cause it to loop forever for non-prime moduli. Internally this function is used when parsing certificates that contain elliptic curve public keys in compressed form or explicit elliptic curve parameters with a base point encoded in compressed form. It is possible to trigger the infinite loop by crafting a certificate that has invalid explicit curve parameters. Since certificate parsing happens prior to verification of the certificate signature, any process that parses an externally supplied certificate may thus be subject to a denial of service attack. The infinite loop can also be reached when parsing crafted private keys as they can contain explicit elliptic curve parameters. Thus vulnerable situations include: - TLS clients consuming server certificates - TLS servers consuming client certificates - Hosting providers taking certificates or private keys from customers - Certificate authorities parsing certification requests from subscribers - Anything else which parses ASN.1 elliptic curve parameters Also any other applications that use the BN_mod_sqrt() where the attacker can control the parameter values are vulnerable to this DoS issue. In the OpenSSL 1.0.2 version the public key is not parsed during initial parsing of the certificate which makes it slightly harder to trigger the infinite loop. However any operation which requires the public key from the certificate will trigger the infinite loop. In particular the attacker can use a self-signed certificate to trigger the loop during verification of the certificate signature. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0. It was addressed in the releases of 1.1.1n and 3.0.2 on the 15th March 2022. Fixed in OpenSSL 3.0.2 (Affected 3.0.0,3.0.1). Fixed in OpenSSL 1.1.1n (Affected 1.1.1-1.1.1m). Fixed in OpenSSL 1.0.2zd (Affected 1.0.2-1.0.2zc).

- Problem Type:
  - CWE-835
- 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, mGuard Device Manager and FL WLAN devices:
https://dam-mdc.phoenixcontact.com/asset/156443151564/d98ef17b0dd8e44798e61a15105a834b/Security_Advisory_CVE-2022-0778.pdf

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

7 Revision History

27 Apr 2022: Initial Publication