Security Advisory
Security routers FL MGUARD and TC MGUARD

1 Advisory Information

Advisory ID: BOSCH-SA-458745
CVE Numbers and Scores:
- CVE-2020-8597
  - CVSS v3.0 Base Score: 9.8 (Critical)

Published: 28 Jul 2020
Last Updated: 28 Jul 2020

2 Summary

The FL MGUARD and TC MGUARD safety devices sold by Bosch Rexroth are devices from Phoenix Contact that have been introduced as commercial goods. A security advisory has been published by the manufacturer, which indicates a critical security vulnerability in the point-to-point services [1].

FL MGUARD, TC MGUARD, TC ROUTER and TC CLOUD CLIENT devices are affected by a buffer overflow vulnerability within the PPP service.
The PPP service is not active by default, but is used commonly at TC ROUTER, TC CLOUD CLIENT.
It is also running in the following FL MGUARD and TC MGUARD configurations:

- Mobile data connection
- Router mode “Modem”
- Router mode “PPPoE”
- L2TP over IPsec

Malicious PPP peers could try to exploit the vulnerability from remote.

3 Affected Products

- R911173814 - FL MGUARD RS4000 TX/TX VPN
- R911173818 - FL MGUARD SMART2 VPN - 2700639
- R911173816 - TC MGUARD RS4000 3G VPN - 2903440
- R911173817 - FL MGUARD DELTA TX/TX - 2700967
- R913058931 - FL MGUARD RS2000 TX/TX-VPN
- R911173815 - TC MGUARD RS2000 3G VPN - 2903441

4 Solution

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

5 Vulnerability Details

5.1 CVE-2020-8597

The version of PPPD shipped with this product has a vulnerability that may allow an unauthenticated remote attacker to cause a stack buffer overflow, which may allow arbitrary code execution on the target system.

- Problem Type:
  - BUFFER COPY WITHOUT CHECKING SIZE OF INPUT ('CLASSIC BUFFER OVERFLOW') CWE-120
- CVSS Vector String: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
  - Base Score: 9.8 (Critical)

6 Additional Resources

[1] Security Advisory for FL MGUARD, TC MGUARD, TC ROUTER and TC CLOUD CLIENT devices
[2] Bosch Rexroth Security Manual Drives and Controls

7 Revision History

28 Jul 2020: Initial Publication