Security Advisory

Denial of Service on Rexroth Fieldbus Couplers

1 Advisory Information

Advisory ID: BOSCH-SA-757244
CVE Numbers and CVSS v3.1 Scores:

- CVE-2025-2813
  - Base Score: 7.5 (High)

Published: 14 Aug 2025
Last Updated: 14 Aug 2025

2 Summary

Several fieldbus couplers sold by Bosch Rexroth contain technology from Phoenix Contact. The manufacturer published a security bulletin about a weakness in the web-based administration interface. A successful attack leads to an overload of the device and the hardware watchdog is triggered. Process data behaves according to the configured substitute value behavior. The bus coupler requires a manual restart (resetting the power supply, pressing the reset button or executing the SNMP reset command) to reestablish communication within the Industrial Ethernet (e.g. PROFINET IO, Modbus/TCP, EtherNet/IP).

3 Affected Products

- Bosch Rexroth AG R-IL ETH BK DI8 DO4 2TX-PAC (R911171726)
  - CVE-2025-2813
    - Version(s): all
- Bosch Rexroth AG S20-EIP-BK (R911173904)
  - CVE-2025-2813
    - Version(s): all
- Bosch Rexroth AG S20-ETH-BK (R911173905)
  - CVE-2025-2813
    - Version(s): < 1.34
- Bosch Rexroth AG S20-PN-BK+ (R911173359)
  - CVE-2025-2813
    - Version(s): all

4 Solution

4.1 Update

A firmware update is available for the **S20-ETH-BK** bus coupler. It is strongly recommended to update to the latest version.

This advisory will be updated when updated firmware versions become available for the other bus couplers.

In the meantime, and in cases where a firmware update is not possible, please refer to the chapter "Compensatory Measures".

4.2 Compensatory Measures

If possible, protect your network by blocking access to port 80 on the affected devices.

If the use of scanners is mandatory for network security in closed production networks, it is recommended to exclude or disable denial of service tests that target port 80.

In general, when using the devices, it is strongly recommended to implement the measures for network segmentation described in the Bosch Rexroth Security Guideline Electric Drives and Controls [1].

5 Vulnerability Details

5.1 CVE-2025-2813

CVE description: An unauthenticated remote attacker can cause a Denial of Service by sending a large number of requests to the http service on port 80.

- 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 Remarks

6.1 CVSS Scoring

Vulnerability classification has been performed using the CVSS v3.1 scoring system. The CVSS environmental score is specific to each customer's environment and should be defined by the customer to attain a final scoring.

7 Additional Resources

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

[2] Third Party Supplier Advisory:
https://assets.phoenixcontact.com/file/f4205726-881c-4184-b010-615e4bea778d/media/original?pcsa-2025-00006_vde-2025-029.pdf

8 Revision History

14 Aug 2025: Initial Publication