Security Advisory

DoS vulnerability on IndraDrive

1 Advisory Information

Advisory ID: BOSCH-SA-315415
CVE Numbers and CVSS v3.1 Scores:

- CVE-2024-48989
  - Base Score: 7.5 (High)

Published: 31 Oct 2024
Last Updated: 31 Oct 2024

2 Summary

A vulnerability in the PROFINET stack implementation of the IndraDrive (all versions) allows an attacker to cause a denial of service, rendering the device unresponsive by sending arbitrary UDP messages.

3 Affected Products

- IndraDrive FWA-INDRV*-MP*
  - CVE-2024-48989
    - Version(s): 17VRS < 20V36

4 Solution

4.1 Update to FWA-INDRV*-MP*-20V36

Starting with FWA-INDRV*-MP*-20V36, the vulnerability has been fixed. Thus, it is recommended, to update your device as soon as possible.

4.2 Compensatory Measures

In use cases in which a device update is not possible or not feasible, compensatory measures are recommended which prevent or at least complicate taking advantage of the vulnerability. Always define such compensatory measures individually, in the context of the operational environment.
Some possible measures are described in the “Security Manual Electric Drives and Controls” [1], for example the network segmentation. In general, it is highly recommended to implement the measures described in the “Security Manual Drives and Controls” [1].

Copyright © 2024 Bosch Rexroth AG

5 Vulnerability Details

5.1 CVE-2024-48989

CVE description: A vulnerability in the PROFINET stack implementation of the IndraDrive (all versions) of Bosch Rexroth allows an attacker to cause a denial of service, rendering the device unresponsive by sending arbitrary UDP messages.

- Problem Type:
  - CWE-400 Uncontrolled Resource Consumption
- 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 Acknowledgement

The vulnerability has been uncovered and disclosed responsibly by **Roni Gavrilov** from **OTORIO**. We thank him for making a responsible disclosure with us.

6.2 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

8 Revision History

31 Oct 2024: Initial Publication

Copyright © 2024 Bosch Rexroth AG