Security Advisory
Denial of Service in Rexroth ActiveMover using Profinet protocol

1 Advisory Information

Advisory ID: Bosch-SA-637429
CVE Numbers and CVSS v3.1 Scores:
- CVE-2021-20986
  - Base Score: 7.5 (High)

Published: 31 Mar 2021
Last Updated: 26 Jan 2022

2 Summary

The ActiveMover with Profinet communication module (Rexroth no. 3842 559 445) sold by Bosch Rexroth contains communication technology from Hilscher (PROFINET IO Device V3) in which a vulnerability with high severity has been discovered [1]. A Denial of Service vulnerability may lead to unexpected loss of cyclic communication or interruption of acyclic communication.

The vulnerability only affects ActiveMover with the Profinet communication module with firmware version below 3.0.32.x. If the product is used in closed (machine) networks with no access to the internet the risk of the vulnerability is very low.

The ActiveMover has a network coupler with a Hilscher protocol stack. This Hilscher protocol stack (PROFINET IO Device V3) does not properly limit available resources when handling Read Implicit Request services, depending on the content of the request. This may lead to shortage of resources so that the affected device
- can no longer perform acyclic requests
- may drop all established cyclic connections
- may disappear completely from the network

3 Affected Products

- Rexroth ActiveMover with firmware version < 3.0.32.x
  with configuration: ‘using Profinet communication module (Rexroth no. 3842 559 445)’

4 Compensatory Measures

There is actually no workaround. However, Bosch Rexroth recommends to operate the product in a closed (machine) network with no access to the internet and implement the following measure:

- Minimize network exposure and ensure that the products are not accessible via the Internet.
- Network segmentation/ Firewall: Isolate affected products from the corporate network.
- If remote access is required, use secure methods such as virtual private networks (VPNs).

With these measures the risk of the vulnerability is very low.

5 Vulnerability Details

5.1 CVE-2021-20986

The Rexroth ActiveMover is affected by CVE-2021-20986.

CVE description: A Denial of Service vulnerability was found in Hilscher PROFINET IO Device V3 in versions prior to V3.14.0.7. This may lead to unexpected loss of cyclic communication or interruption of acyclic communication.

- Problem Type:
  - CWE-121 Stack-based Buffer Overflow
- CVSS Vector String: CVSS:3.0/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] Hilscher Security Advisory:
https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device

7 Revision History

26 Jan 2022: Add firmware version
31 Mar 2021: Initial Publication