Security Advisory
Denial of Service in Rexroth ActiveMover using EtherNet/IP protocol

1 Advisory Information

Advisory ID: BOSCH-SA-282922
CVE Numbers and CVSS v3.1 Scores:
- CVE-2021-20987
  - Base Score: 7.5 (High)

Published: 31 Mar 2021
Last Updated: 31 Mar 2021

2 Summary

The ActiveMover with the EtherNet/IP communication module (Rexroth no. 3842 559 444) sold by Bosch Rexroth contains communication technology from Hilscher (EtherNet/IP Core V2) in which a vulnerability with high severity has been discovered [1]. A denial of service and memory corruption vulnerability could allow arbitrary code to be injected through the network or make the EtherNet/IP device crash without recovery.

The vulnerability only affects ActiveMover with firmware versions below 3.0.26.x using the EtherNet/IP communication module. If the product is used in closed (machine) networks with no access to the internet the risk of the vulnerability is very low.

Hilscher's EtherNet/IP Core V2 processes a CIP service request that is received from the network. During that process the attached service data is copied into an internal buffer without checking the size of the data being copied. This results in memory corruption (stack damage) that could be used for remote code injection. In addition, the EtherNet/IP device stops responding due to its corrupted stack, making it vulnerable to a denial-of-service attack.

3 Affected Products

- Rexroth ActiveMover < 3.0.26.x
  with configuration: 'using EtherNet/IP communication module (Rexroth no. 3842 559 444)'

4 Compensatory Measures

ActiveMover firmware version 3.0.26.x and higher is not affected. For versions below 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-2021-20987

The Rexroth ActiveMover prior to version 3.0.26.x is affected by CVE-2021-20987.

CVE description: A denial of service and memory corruption vulnerability was found in Hilscher EtherNet/IP Core V2 prior to V2.13.0.21that may lead to code injection through network or make devices crash without recovery.

- 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 Cyber Security website and the corresponding advisory:
https://kb.hilscher.com/pages/viewpage.action?pageId=108969480

7 Revision History

31 Mar 2021: Initial Publication