Security Advisory
Denial of Service in Rexroth ID 200/C-ETH using EtherNet/IP Protocol

1 Advisory Information

Advisory ID: BOSCH-SA-775371
CVE Numbers and CVSS v3.1 Scores:
- CVE-2020-25159
  - Base Score: 9.8 (Critical)

Published: 27 Jan 2021
Last Updated: 27 Jan 2021

2 Summary

The ID 200/C-ETH (Rexroth No. 3842 410 060) sold by Bosch Rexroth contains communication technology (499ES EtherNet/IP) from Real Time Automation (RTA) in which a critical vulnerability has been discovered. By exploiting the vulnerability, an attacker can send a specially crafted packet that may result in a denial-of-service condition or code execution.

The vulnerability only affects ID 200/C-ETH used in combination with the Ethernet/IP protocol. If the product is used in closed (machine) networks with no access to the internet the risk of the vulnerability is very low. The Usage of the ID 200/C-ETH with PROFINET, MODBUS, TCP/IP protocol is NOT affected.

3 Affected Products

Rexroth ID 200/C-ETH with configuration: ‘using the EtherNet/IP Protocol’

4 Solution and Mitigations

4.1 Operate the product in a closed environment

For the use of ID 200/C-ETH in combination with the Ethernet/IP protocol, 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).

5 Vulnerability Details

5.1 CVE-2020-25159

Rexroth ID 200/C-ETH using EtherNet/IP protocol is affected by CVE-2020-25159. Remote attackers may exploit the vulnerability to get access to the device and execute any program and tap information.

CVE description: 499ES EtherNet/IP (ENIP) Adaptor Source Code is vulnerable to a stack-based buffer overflow, which may allow an attacker to send a specially crafted packet that may result in a denial-of-service condition or code execution.

- Problem Type:
  - STACK-BASED BUFFER OVERFLOW CWE-121
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 9.8 (Critical)

6 Revision History

27 Jan 2021: Initial Publication