Denial-of-Service (DoS) Vulnerabilities in simulation function of GX Works2

Release date: November 21, 2023
Mitsubishi Electric Corporation

Overview

Denial-of-service (DoS) vulnerabilities due to improper input validation (CWE-20[1]) exist in simulation function of GX Works2. An attacker may be able to cause denial-of-service (DoS) condition on the function by sending specially crafted packets (CVE-2023-5274, CVE-2023-5275). However, the attacker would need to send the packets from within the same personal computer where the function is running.

CVSS[2]

CVE-2023-5274 CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:L Base Score:2.5
CVE-2023-5275 CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:L Base Score:2.5

Affected products

The following products are affected:
< Products and Versions >
- GX Works2, all versions

<How to Check the Versions>
- GX Works2 : Please refer "GX Works2 Version 1 Operating Manual (Common)" – "3.4 Help Function" – "3.4.4 Checking version of GX Works2".

Description

Denial-of-service (DoS) vulnerabilities due to improper input validation (CWE-20) exist in simulation function of GX Works2.

Impact

An attacker may be able to cause denial-of-service (DoS) condition on the function by sending specially crafted packets. However, the attacker would need to send the packets from within the same personal computer where the function is running.

Countermeasures

Please carry out mitigations/workarounds.

Mitigations / Workarounds

Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting this vulnerability:
- Install an antivirus software in your personal computer using the affected product.
- Use your personal computer with the affected product within the LAN and block remote login from untrusted networks, hosts, and users.
- When connecting your personal computer with the affected product to the Internet, use a firewall, virtual private network (VPN), etc., to prevent unauthorized access, and allow only trusted users to remote login.
- Don't open untrusted files or click untrusted links.

Acknowledgement

Mitsubishi Electric would like to thank joker63 of ZheJiangQiAnTechnology who reported this vulnerability.

Contact information

Please contact your local Mitsubishi Electric representative.
<Inquiries | MITSUBISHI ELECTRIC FA>
https://www.mitsubishielectric.com/fa/support/index.html

[1] https://cwe.mitre.org/data/definitions/20.html
[2] https://www.first.org/cvss/v3.1/specification-document