Malicious Code Execution Vulnerability in FA Engineering Software Products

Release date: September 19, 2023
Mitsubishi Electric Corporation

Overview

Malicious Code Execution Vulnerability due to Incorrect Default Permissions (CWE-276[1]) exists in Multiple FA engineering software products because of incomplete fix to address CVE-2020-14496[2].

This vulnerability could allow a malicious local attacker to execute a malicious code, which could result in information disclosure, tampering with and deletion, or a denial-of-service (DoS) condition.

However, if the mitigated version described in the advisory for CVE-2020-14496 is used and installed in the default installation folder, this vulnerability does not affect the products.

The product names and versions affected by the vulnerability are listed below.

CVSS[3]

CVE-2023-4088 CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H Base Score:9.3

Affected products

< Products and Versions >
- GX Works3, all versions

<How to Check the Versions>
- GX Works3 : Please refer "GX Works3 Operating Manual" – "1.8 Learning Operation Methods of GX Works3" – "Checking the version of GX Works3".

Description

Malicious Code Execution Vulnerability due to Incorrect Default Permissions (CWE -276) exists in Multiple FA engineering software products.

However, if the mitigated version described in the advisory for CVE-2020-14496 is used and installed in the default installation folder, this vulnerability does not affect the products.

Impact

This vulnerability could allow a malicious local attacker to execute a malicious code, which could result in information disclosure, tampering with and deletion, or a denial-of-service (DoS) condition.

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 the mitigated version described in the advisory for CVE-2020-14496 into the default installation folder. If it is necessary to change the installation folder from the default, select a folder that only users with Administrator privileges have permission to change.
- 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 perconal 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 01dGu0 of ZHEJIANG QIAN INFORMATION & TECHNOLOGY CO., LTD. who reported this vulnerability.

[1] https://cwe.mitre.org/data/definitions/276.html
[2] https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2020-006_en.pdf
[3] https://www.first.org/cvss/v3.1/specification-document

Contact information

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