Malicious Code Execution Vulnerability in Multiple FA Engineering Software Products

Release date: November 30, 2023
Mitsubishi Electric Corporation

Overview

Malicious Code Execution Vulnerability due to External Control of File Name or Path (CWE-73[1]) exists in Multiple FA engineering software products.

This vulnerability could allow a malicious attacker to execute a malicious code by having legitimate users open a specially crafted project file, which could result in information disclosure, tampering and deletion, or a denial-of-service (DoS) condition (CVE-2023-5247).

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

CVSS[2]

CVE-2023-5247 CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H Base Score:7.8

Affected products

< Products and Versions >

Product name	Versions
GX Works3	All versions
MELSOFT iQ AppPortal	All versions
MELSOFT Navigator	All versions
Motion Control Setting (*1)	All versions

(*1) Software packaged with GX Works3

<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”.
- MELSOFT iQ AppPortal : Please refer “iQ AppPortal Operation Manual” – “1.4 Learning Operation Methods of iQ AppPortal” – “Checking the version of iQ AppPortal”.
- MELSOFT Navigator : Please refer “MELSOFT Navigator Version2 Help” – “2 Screen Structure and Basic Operation” – “9.3 Check Version Information of MELSOFT Navigator”.
- Motion Control Setting : Please refer “Motion Control Setting Function Help” – “1.2 Learning Operation Methods of Motion Control Setting Function” – “Checking the version of Motion Control Setting Function”

Description

Malicious Code Execution Vulnerability (CVE-2023-5247) due to External Control of File Name or Path (CWE-73) exists in multiple FA engineering software products.

Impact

This vulnerability could allow a malicious attacker to execute a malicious code by having legitimate users open a specially crafted project file, which could result in information disclosure, tampering 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 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.

[1] https://cwe.mitre.org/data/definitions/73.html
[2] https://www.first.org/cvss/v3.1/specification-document

Acknowledgement

Mitsubishi Electric would like to thank 01dGu0 of ZHEJIANG QIAN INFORMATION & TECHNOLOGY CO., LTD. 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