# Multiple Vulnerabilities in Multiple FA Engineering Software

Release date: November 24, 2022
Last update date: December 12, 2023
Mitsubishi Electric Corporation

## ■Overview

Multiple vulnerabilities exist in multiple Mitsubishi Electric FA engineering software. If these vulnerabilities are exploited by malicious attackers, disclosure or tampering of the product's information could allow unauthorized users to gain access to the MELSEC iQ-R/F/L series CPU modules, and MELSEC iQ-R series OPC UA server module, to view and execute programs, or to view project file illegally. (CVE-2022-25164, CVE-2022-29825, CVE-2022-29826, CVE-2022-29827, CVE-2022-29828, CVE-2022-29829, CVE-2022-29830, CVE-2022-29831, CVE-2022-29832, CVE-2022-29833)

## ■CVSS[1]

| | | |
|---|---|---|
| CVE-2022-25164 | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N | Base Score:8.6 |
| CVE-2022-29825 | CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N | Base Score:5.6 |
| CVE-2022-29826 | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N | Base Score:6.8 |
| CVE-2022-29827 | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N | Base Score:6.8 |
| CVE-2022-29828 | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N | Base Score:6.8 |
| CVE-2022-29829 | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N | Base Score:6.8 |
| CVE-2022-29830 | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N | Base Score:9.1 |
| CVE-2022-29831 | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N | Base Score:7.5 |
| CVE-2022-29832 | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N | Base Score:3.7 |
| CVE-2022-29833 | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:H/A:N | Base Score:6.8 |

[1] https://www.first.org/cvss/v3.1/specification-document

■Affected products

<Products and Versions>

| No. | Product Name | Version | Applicable CVE ID |
|---|---|---|---|
| 1 | GX Works3 | from 1.000A to 1.011M | CVE-2022-25164<br>CVE-2022-29825<br>CVE-2022-29826<br>CVE-2022-29827<br>CVE-2022-29828<br>CVE-2022-29829<br>CVE-2022-29830 |
| | | from 1.015R to 1.087R | CVE-2022-25164<br>CVE-2022-29825<br>CVE-2022-29826<br>CVE-2022-29827<br>CVE-2022-29828<br>CVE-2022-29829<br>CVE-2022-29830<br>CVE-2022-29831<br>CVE-2022-29832<br>CVE-2022-29833 |
| | | 1.090U | CVE-2022-25164<br>CVE-2022-29825<br>CVE-2022-29827<br>CVE-2022-29828<br>CVE-2022-29829<br>CVE-2022-29830<br>CVE-2022-29831<br>CVE-2022-29832<br>CVE-2022-29833 |
| | | 1.095Z | CVE-2022-25164<br>CVE-2022-29827<br>CVE-2022-29828<br>CVE-2022-29830<br>CVE-2022-29831<br>CVE-2022-29832<br>CVE-2022-29833 |
| | | 1.096A and later | CVE-2022-29827<br>CVE-2022-29828<br>CVE-2022-29832<br>CVE-2022-29833 |
| 2 | MX OPC UA Module Configurator-R | 1.08J and prior | CVE-2022-25164 |
| 3 | GX Works2 | all versions | CVE-2022-29832 |
| 4 | GX Developer | 8.40S and later | CVE-2022-29832 |
| 5 | GT Designer3 Version1 (GOT2000) | from 1.122C to 1.290C | CVE-2022-29825<br>CVE-2022-29829 |
| 6 | Motion Control Setting(*1) | from 1.000A to 1.033K | CVE-2022-29826<br>CVE-2022-29830 |
| | | from 1.035M to 1.042U | CVE-2022-29826<br>CVE-2022-29829<br>CVE-2022-29830 |
| | | 1.045X and later | CVE-2022-29830 |

(*1) GX Works3 related software

<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”.
- MX OPC UA Module Configurator-R : Please refer ″2.12 Help″ in the MELSEC iQ-R OPC UA Server Module User's Manual (Application).
- GX Works2 : Please refer “GX Works2 Version 1 Operating Manual (Common)” - “3.4.4 Checking version of GX Works2”.
- GX Developer : Please refer “GX Developer Version 8 Operating Manual” - “15.17 Outline of Help Function”.
- GT Designer3 Version1 (GOT2000) : Please refer “GT Designer3(GOT2000) Screen Design Manual” - “2.2.1 Menus” - “13 [Help]”.
- 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”.

< How to Obtain Manuals >

The latest manuals for software products can be downloaded from the following site:
https://www.mitsubishielectric.com/fa/#software

## ■Description

Vulnerabilities below exist in multiple Mitsubishi Electric FA engineering software.

CVE-2022-25164 : Information disclosure vulnerability due to Cleartext Storage of Sensitive Information (CWE-312)[2]

CVE-2022-29825 : Information disclosure vulnerability due to Use of Hard-coded Password (CWE-259)[3]

CVE-2022-29826 : Information disclosure vulnerability due to Cleartext Storage of Sensitive Information (CWE-312)

CVE-2022-29827 : Information disclosure vulnerability due to Use of Hard-coded Cryptographic Key (CWE-321)[4]

CVE-2022-29828 : Information disclosure vulnerability due to Use of Hard-coded Cryptographic Key (CWE-321)

CVE-2022-29829 : Information disclosure vulnerability due to Use of Hard-coded Cryptographic Key (CWE-321)

CVE-2022-29830 : Information disclosure and information tampering vulnerability due to Use of Hard-coded Cryptographic Key (CWE-321)

CVE-2022-29831 : Information disclosure vulnerability due to Use of Hard-coded Password (CWE-259)

CVE-2022-29832 : Information disclosure vulnerability due to Cleartext Storage of Sensitive Information in Memory (CWE-316)[5]

CVE-2022-29833 : Information disclosure vulnerability due to Insufficiently Protected Credentials (CWE-522)[6]

## ■Impact

CVE-2022-25164:

If this vulnerability is exploited, sensitive information may be disclosed. As a result, unauthorized users can gain unauthorized access to the CPU module and the OPC UA server module.

CVE-2022-29825, CVE-2022-29826, CVE-2022-29827, CVE-2022-29828, CVE-2022-29829:

If these vulnerabilities are exploited, sensitive information may be disclosed. As a result, unauthorized users may view programs and project files or execute programs illegally.

CVE-2022-29830:

If this vulnerability is exploited, sensitive information may be disclosed or tampered. As a result, information about project files can be obtained illegally by unauthorized users.

CVE-2022-29831:

If this vulnerability is exploited, unauthorized users could obtain information about the project file for the safety CPU module.

CVE-2022-29832:

If this vulnerability is exploited, sensitive information may be disclosed. As a result, unauthorized users could obtain information about the project file for the safety CPU module or project file for MELSEC Q/FX/L series with security setting.

CVE-2022-29833:

If this vulnerability is exploited, sensitive information may be disclosed. As a result, unauthorized users could access to the safety CPU module illgally.

## ■Countermeasures

The table below shows countermeasures for each vulnerability.

For customers who are using products with no description of countermeasures (GX Works2 and GX Developer) or who are not able to immediately update the products, please take mitigations or workarounds

To update to a fixed version, refer to <How to Get the Fixed Versions> and <How to Update>.

[2] https://cwe.mitre.org/data/definitions/312.html

[3] https://cwe.mitre.org/data/definitions/259.html

[4] https://cwe.mitre.org/data/definitions/321.html

[5] https://cwe.mitre.org/data/definitions/316.html

[6] https://cwe.mitre.org/data/definitions/522.html

| No. | Product Name | Applicable CVE ID | Countermeasure |
|---|---|---|---|
| 1 | GX Works3 | CVE-2022-29826 | Download fixed Ver. 1.090U or later and update the software. |
| | | CVE-2022-29825<br>CVE-2022-29829 | Download fixed Ver. 1.095Z or later and update the software. Then set security key's secure mode enable.<br>Please refer "GX Works3 Operating Manual" - "15.2 Preventing Illegal Access to Programs (Security Key)" in detail. |
| | | CVE-2022-25164<br>CVE-2022-29830<br>CVE-2022-29831 | Download fixed Ver. 1.096A or later and update the software. Please set serurity version to "2".<br>Please refer "GX Works3 Operating Manual" - "15.8 Preventing Illegal Access to/Falsification of Data (Security Version)" in detail. |
| | | CVE-2022-29827<br>CVE-2022-29828<br>CVE-2022-29832<br>CVE-2022-29833 | Please take mitigations and workarounds. |
| 2 | MX OPC UA Module Configurator-R | CVE-2022-25164 | Download fixed Ver. 1.09K or later and update the software.<br>Also, update the firmware version of the OPC UA server module to 10 or later. |
| 3 | GT Designer3 Version1 (GOT2000) | CVE-2022-29825<br>CVE-2022-29829 | Download fixed Ver. 1.295H or later and update the software. Then set security key's secure mode enable.<br>Please refer "GT Designer3(GOT2000) Screen Design Manual" - "2.12 Protecting a Project with a Security Key " - "2.12.5 [Security Key Management] dialog" - "[Switch Secure Mode] dialog" in detail. |
| 4 | Motion Control Setting | CVE-2022-29826 | Download fixed Ver. 1.045X or later and update the software.<br>Please take the countermeasure for CVE-2022-29826 of No.1 GX Works3 in this table. |
| | | CVE-2022-29829 | Download fixed Ver. 1.045X or later and update the software.<br>Please take the countermeasure for CVE-2022-29829 of No.1 GX Works3 in this table. |
| | | CVE-2022-29830 | Please take mitigations and workarounds. |

<How to Get the Fixed Versions>
Download the latest version of the software from the following site and update the software.
https://www.mitsubishielectric.com/fa/#software

<How to Update>
1. Unzip the downloaded file (zip format).
2. Execute the file "setup.exe" in the unzipped folder to install.

■Mitigations/Workarounds

Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of being exploited these vulnerabilities:

| Applicable CVE ID | Mitigations or Workarounds |
|---|---|
| CVE-2022-25164 | - Make sure that malicious attackers cannot access project files or security keys that are stored in your computer/server and configuration files that are stored in your personal computer running the software, via untrusted network or host<br>- Install an antivirus software in your personal computer running the software.<br>- Encrypt project files and security keys when sending or receiving them over the Internet.<br>- Use the "authentication with a certificate" function instead of "username / password authentication" for user authentication for access from OPC UA clients to MELSEC iQ-R series OPC UA server modules. (MX OPC UA Module Configurator-R only) |
| CVE-2022-29825 | - Make sure that malicious attackers cannot access project files or security keys that are stored in your computer/server and configuration files that are stored in your personal computer running the software, via untrusted network or host<br>- Install an antivirus software in your personal computer running the software. |
| CVE-2022-29826<br>CVE-2022-29827<br>CVE-2022-29828<br>CVE-2022-29829<br>CVE-2022-29830<br>CVE-2022-29831<br>CVE-2022-29832<br>CVE-2022-29833 | - Make sure that malicious attackers cannot access project files or security keys that are stored in your computer/server and configuration files that are stored in your personal computer running the software, via untrusted network or host<br>- Install an antivirus software in your personal computer running the software.<br>- Encrypt project files and security keys when sending or receiving them over the Internet. |

## ■Acknowledgements

Mitsubishi Electric would like to thank people below.

CVE-2022-25164: Anton Dorfman and Vladimir Nazarov, of Positive Technologies
CVE-2022-29825: Anton Dorfman and Dmitry Sklyarov, of Positive Technologies
CVE-2022-29826: Anton Dorfman and Iliya Rogachev, of Positive Technologies
CVE-2022-29827: Dmitry Sklyarov and Anton Dorfman, of Positive Technologies
CVE-2022-29828: Dmitry Sklyarov and Anton Dorfman, of Positive Technologies
CVE-2022-29829: Dmitry Sklyarov and Anton Dorfman, of Positive Technologies
CVE-2022-29830: Dmitry Sklyarov and Anton Dorfman, of Positive Technologies
CVE-2022-29831: Ivan Speziale of Nozomi Networks
CVE-2022-29832: Ivan Speziale of Nozomi Networks
CVE-2022-29833: Ivan Speziale of Nozomi Networks

## ■Contact information

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

## ■Update history

December 12, 2023
- GX Works2 and GX Developer, those are not planned to be fixed, have been added to “Countermeasures”.

June 29, 2023
- The affected versions of following products have been modified in “Affected products”.
  GX Works3, MX OPC UA Module Configurator-R
- Countermeasure information for GX Works3 has been added to “Countermeasures”.
- MX OPC UA Module Configurator-R has been added to “Countermeasures”.

May 30, 2023
- The following products have been added to ″Affected products″.
  GX Works2
  GX Developer
  GT Designer3 Version1 (GOT2000)
  Motion Control Setting
- In line with the above, ″Overview″ and ″ Impact″ have been revised.
- Overview of each vulnerability have been added to the “Description”.
- Fixed products have been added to “Countermeasures”.