Multiple Vulnerabilities in Multiple FA Engineering Software

Release date: November 24, 2022
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 or to view and execute programs 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	1.000A or later and 1.011M and prior	CVE-2022-25164 CVE-2022-29825 CVE-2022-29826 CVE-2022-29827 CVE-2022-29828 CVE-2022-29829 CVE-2022-29830
		1.015R or later and 1.086Q and prior	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
		1.087R or later	CVE-2022-25164 CVE-2022-29825 CVE-2022-29827 CVE-2022-29828 CVE-2022-29829 CVE-2022-29830 CVE-2022-29831 CVE-2022-29832 CVE-2022-29833
2	MX OPC UA Module Configurator-R	all versions	CVE-2022-25164

<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).

< How to Obtain Manuals >

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

■Description

Multiple vulnerabilities below exist in multiple Mitsubishi Electric FA engineering software.
CVE-2022-25164 : Cleartext Storage of Sensitive Information （CWE-312）[2]
CVE-2022-29825 : Use of Hard-coded Password (CWE-259)[3]
CVE-2022-29826 : Cleartext Storage of Sensitive Information (CWE-312)
CVE-2022-29827 : Use of Hard-coded Cryptographic Key (CWE-321)[4]
CVE-2022-29828 : Use of Hard-coded Cryptographic Key (CWE-321)
CVE-2022-29829 : Use of Hard-coded Cryptographic Key (CWE-321)
CVE-2022-29830 : Use of Hard-coded Cryptographic Key (CWE-321)
CVE-2022-29831 : Use of Hard-coded Password (CWE-259)
CVE-2022-29832 : Cleartext Storage of Sensitive Information in Memory (CWE-316)[5]
CVE-2022-29833 : Insufficiently Protected Credentials (CWE-522)[6]

[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

■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 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.

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 products with no description of countermeasures, please take mitigations or workarounds

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

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-2022-25164 CVE-2022-29825 CVE-2022-29829 CVE-2022-29830 CVE-2022-29831	Fixed version will be released near the future. Please take mitigations and workarounds until the fixed version is released.
		CVE-2022-29827 CVE-2022-29828 CVE-2022-29832 CVE-2022-29833	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 - Install an antivirus software in your personal computer running the software. - Encrypt project files and security keys when sending or receiving them over the Internet. - 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 - Install an antivirus software in your personal computer running the software.
CVE-2022-29826 CVE-2022-29827 CVE-2022-29828 CVE-2022-29829 CVE-2022-29830 CVE-2022-29831 CVE-2022-29832 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 - Install an antivirus software in your personal computer running the software. - 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