Multiple Vulnerabilities due to Vulnerabilities in Jungo's WinDriver in Multiple FA Engineering Software Products

Release date: May 14, 2024
Last update date: September 1, 2026
Mitsubishi Electric Corporation

Overview

Multiple vulnerabilities due to vulnerabilities in Jungo's WinDriver exist in multiple FA engineering software products. If a malicious code is executed on a computer where the affected software product is installed, these vulnerabilities may allow a local attacker to cause a Windows blue screen (BSOD) error that results in a denial of service (DoS) condition and/or to gain Windows system privileges and execute arbitrary commands (CVE-2023-51776, CVE-2023-51777, CVE-2023-51778, CVE-2024-22102, CVE-2024-22103, CVE-2024-22104, CVE-2024-22105, CVE-2024-22106, CVE-2024-25086, CVE-2024-25087, CVE-2024-25088, CVE-2024-26314). However, attacks against these vulnerabilities can be detected by Microsoft Windows Defender.

CVSS[1]

CVE-2023-51776	CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:N/I:H/A:N	Base Score:4.4
CVE-2023-51777	CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:N/I:N/A:H	Base Score:4.4
CVE-2023-51778	CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:N/I:N/A:H	Base Score:4.4
CVE-2024-22102	CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:N/I:N/A:H	Base Score:4.4
CVE-2024-22103	CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:N/I:N/A:H	Base Score:4.4
CVE-2024-22104	CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:N/I:N/A:H	Base Score:4.4
CVE-2024-22105	CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:N/I:N/A:H	Base Score:4.4
CVE-2024-22106	CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:N/I:H/A:H	Base Score:6.0
CVE-2024-25086	CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:N/I:H/A:N	Base Score:4.4
CVE-2024-25087	CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:N/I:N/A:H	Base Score:4.4
CVE-2024-25088	CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:N/I:H/A:N	Base Score:4.4
CVE-2024-26314	CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:N/I:H/A:N	Base Score:4.4

Affected products

The affected products and versions are as follows.

Product name	Version
CPU Module Logging Configuration Tool	"1.154L" and prior
CSGL (GX Works2 connection configuration)	"2.5" and prior
CW Configurator	"1.019V" and prior
Data Transfer	"3.58L" and prior
Data Transfer Classic	"1.00A" and prior
EZSocket (*1)	"5.92" and prior
FR Configurator SW3	All versions
FR Configurator2	"1.32J" and prior
GENESIS64 and ICONICS Suite	“10.97.1” to "10.97.3"
GT Designer3 Version1 (GOT1000)	"1.310Y" and prior
GT Designer3 Version1 (GOT2000)	"1.317F" and prior
GT SoftGOT1000 Version3	"3.310Y" and prior
GT SoftGOT2000 Version1	"1.315D" and prior
GX Developer	All versions
GX LogViewer	"1.154L" and prior
GX Works2	"1.622Y" and prior
GX Works3	"1.106L" and prior
iQ Works (MELSOFT Navigator)	"2.102G" and prior
MI Configurator	All versions
Mitsubishi Electric Numerical Control Device Communication Software (FCSB1224)	"A8" and prior
MR Configurator (SETUP221)	All versions
MR Configurator2	"1.150G" and prior
Position Board Utility2(MRZJW3-MC2-UTL)	"3.40" and prior
MX Component	"5.007H" and prior
MX OPC Server DA/UA (Software packaged with MC Works64)	All versions
PX Developer/Monitor Tool	"1.58L " and prior
RT ToolBox3	"2.20W" and prior
RT VisualBox	"1.11M " and prior

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

Setting/monitoring tools for the C Controller module (SW4PVC-CCPU)	"4.14Q" and prior
MELSECNET/H Interface Board software package (SW0DNC-MNETH-B)	"36N" and prior
CC-Link System Master/Local Interface Board software package (SW1DNC-CCBD2-B)	"1.25B" and prior
CC-Link IE Field Network Interface Board software package (SW1DNC-CCIEF-J/-B)	"1.18U" and prior
CC-Link IE Controller Network Interface Board software package (SW1DNC-MNETG-B)	"1.31H" and prior
C Controller Interface Module utility (SW1DNC-QSCCF-B)	"2.10" and prior
MELSOFT EM Software Development Kit (SW1DND-EMSDK-B)	"1.020W" and prior
MT Works2	"1.200J " and prior

(*1) EZSocket is a communication middleware product for Mitsubishi Electric partner companies.

<How to Check the Versions>
Please refer to the manual or help documentation for each product.

Description

The following multiple vulnerabilities due to vulnerabilities in Jungo's WinDriver exist in multiple FA engineering software products. However, attacks against these vulnerabilities can be detected by Microsoft Windows Defender.

CVE ID	Description of the vulnerabilities
CVE-2023-51776	Privilege escalation vulnerability due to Improper Privilege Management (CWE-269[2])
CVE-2023-51777	Denial of Service (DoS) vulnerability due to Uncontrolled Resource Consumption (CWE-400[3])
CVE-2023-51778	Denial of Service (DoS) vulnerability due to Out-of-bounds Write (CWE-787[4])
CVE-2024-22102	Denial of Service (DoS) vulnerability due to Uncontrolled Resource Consumption (CWE-400)
CVE-2024-22103	Denial of Service (DoS) vulnerability due to Out-of-bounds Write (CWE-787)
CVE-2024-22104	Denial of Service (DoS) vulnerability due to Out-of-bounds Write (CWE-787)
CVE-2024-22105	Denial of Service (DoS) vulnerability due to Uncontrolled Resource Consumption (CWE-400)
CVE-2024-22106	Privilege escalation and Denial of Service (DoS) vulnerability due to Improper Privilege Management (CWE-269)
CVE-2024-25086	Privilege escalation vulnerability due to Improper Privilege Management (CWE-269)
CVE-2024-25087	Denial of Service (DoS) vulnerability due to Uncontrolled Resource Consumption (CWE-400)
CVE-2024-25088	Privilege escalation vulnerability due to Improper Privilege Management (CWE-269)
CVE-2024-26314	Privilege escalation vulnerability due to Improper Privilege Management (CWE-269)

Impact

[CVE-2023-51777, CVE-2023-51778, CVE-2024-22102, CVE-2024-22103, CVE-2024-22104, CVE-2024-22105, CVE-2024-25087]
If a malicious code is executed on a computer where the affected software product is installed, these vulnerabilities may allow a local attacker to cause a Windows blue screen (BSOD) error that results in a denial of service (DoS) condition.

[CVE-2023-51776, CVE-2024-25086, CVE-2024-25088, CVE-2024-26314]
If a malicious code is executed on a computer where the affected software product is installed, these vulnerabilities may allow a local attacker to gain Windows system privileges and execute arbitrary commands.

[CVE-2024-22106]
If a malicious code is executed on a computer where the affected software product is installed, these vulnerabilities may allow a local attacker to cause a Windows blue screen (BSOD) error that results in a denial of service (DoS) condition and/or to gain Windows system privileges and execute arbitrary commands.

2 https://cwe.mitre.org/data/definitions/269.html
3 https://cwe.mitre.org/data/definitions/400.html
4 https://cwe.mitre.org/data/definitions/787.html

Countermeasures for Customers

- Customers using the affected products for which countermeasure versions are listed in "Countermeasures for Products"
  Please download and install the update from the following site.
  https://www.mitsubishielectric.com/fa/download/index.html

  We do not provide downloadable updates for the following products. Please contact your place of purchase for assistance.
  EZSocket
  CSGL (GX Works2 connection configuration)
  Position Board Utility2(MRZJW3-MC2-UTL)
  C Controller Interface Module utility (SW1DNC-QSCCF-B)

  We recommend that customers using GENESIS64 and ICONICS Suite consider replacing them with the successor product, GENESIS.

- Customers using the affected products for which countermeasure versions are not listed in "Countermeasures for Products"
  Please take the following “Mitigations/Workarounds”.

  Please note that there are no plans to release fixed versions of the following product:
  FR Configurator SW3
  GX Developer
  MI Configurator
  MR Configurator (SETUP221)
  MX OPC Server DA/UA (Software packaged with MC Works64)

Countermeasures for Products

The following products have been fixed multiple vulnerabilities due to vulnerabilities in Jungo's WinDriver.

Product name	Version
CPU Module Logging Configuration Tool	"1.160S" or later
CSGL (GX Works2 connection configuration)	"2.6" or later
CW Configurator	"1.020W" or later
Data Transfer	"3.59M" or later
Data Transfer Classic	"1.01B" or later
EZSocket (*1)	"5.A" or later
FR Configurator2	"1.33K" or later
GENESIS64 and ICONICS Suite	"10.98" or later
GT Designer3 Version1 (GOT1000)	"1.315D" or later
GT Designer3 Version1 (GOT2000)	"1.320J" or later
GT SoftGOT1000 Version3	"3.315D" or later
GT SoftGOT2000 Version1	"1.320J" or later
GX LogViewer	"1.160S" or later
GX Works2	"1.625B" or later
GX Works3	"1.110Q" or later
iQ Works (MELSOFT Navigator)	"2.106L" or later
Mitsubishi Electric Numerical Control Device Communication Software (FCSB1224)	"A9" or later
MR Configurator2	"1.155M" or later
Position Board Utility2(MRZJW3-MC2-UTL)	"3.50" or later
MX Component	"5.008J" or later
PX Developer/Monitor Tool	"1.59M" or later
RT ToolBox3	"2.50C" or later
RT VisualBox	"1.12N" or later
Setting/monitoring tools for the C Controller module (SW4PVC-CCPU)	"4.15R" or later
MELSECNET/H Interface Board software package (SW0DNC-MNETH-B)	"37P" or later
CC-Link System Master/Local Interface Board software package (SW1DNC-CCBD2-B)	"1.26C" or later
CC-Link IE Field Network Interface Board software package (SW1DNC-CCIEF-J/-B)	"1.19V" or later
CC-Link IE Controller Network Interface Board software package (SW1DNC-MNETG-B)	"1.32J" or later
C Controller Interface Module utility (SW1DNC-QSCCF-B)	"2.20" or later
MELSOFT EM Software Development Kit (SW1DND-EMSDK-B)	"1.025B" or later
MT Works2	"1.205P" or later

Mitigations / Workarounds

If continued use of a vulnerable version of GENESIS64 or ICONICS Suite is required and communication with Mitsubishi Electric devices is not necessary, Mitsubishi Electric recommends not installing the Mitsubishi Electric FA Connector component during software installation as a workaround for this issue. For existing systems, removal of the Mitsubishi Electric FA Connector component

is not supported. To apply this workaround, the software must be installed on a new or formatted system without the Mitsubishi Electric FA Connector component.

Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting these vulnerabilities:
- Restrict physical access to the computer using the product.
- Install antivirus software in your computer using the affected product.
- Don’t open untrusted files or click untrusted links.

Acknowledgement

Mitsubishi Electric would like to thank Jongseong Kim, Byunghyun Kang, Sangjun Park, Yunjin Park, Kwon Yul, Seungchan Kim (today-0day, BoB 12th) who reported these vulnerabilities.

Contact information

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

Update history

September 1, 2026
Updated the version of the following products to the "Affected Products" section.
GENESIS64 and ICONICS Suite
Added description regarding GENESIS64 and the ICONICS Suite to the "Countermeasures for Customers" section.
Added the updated products to the "Countermeasures for Products" section.
GENESIS64 and ICONICS Suite
Added a workaround to the “Mitigations / Workarounds” section.

January 15, 2026
Added the following products to the "Affected Products" section.
ICONICS Suite
MT Works2
Added the updated products to the "Countermeasures for Products" section.
GENESIS
Mitsubishi Electric Numerical Control Device Communication Software (FCSB1224)
PX Developer/Monitor Tool
RT VisualBox
C Controller Interface Module utility (SW1DNC-QSCCF-B)
MT Works2

August 28, 2025
Added the updated products to the "Countermeasures for Products" section.
CW Configurator
Setting/monitoring tools for the C Controller module (SW4PVC-CCPU)
MELSOFT EM Software Development Kit (SW1DND-EMSDK-B)

May 15, 2025
Added products for which there are no plans to release fixed versions to the "Countermeasures for Customers" section.
Added the updated products to the "Countermeasures for Products" section.
Position Board Utility2(MRZJW3-MC2-UTL)

January 30, 2025
Added the response method for products that do not provide downloadable updates to the "Countermeasures for Customers" section.
Added the updated products to the "Countermeasures for Products" section.
CPU Module Logging Configuration Tool
CSGL (GX Works2 connection configuration)
EZSocket
FR Configurator2
GX LogViewer
GX Works2
GX Works3
iQ Works (MELSOFT Navigator)
MX Component

October 31, 2024

In the "Affected Products" section, the following product names have been revised.

Position Board Utility2(MRZJW3-MC2-UTL)

MELSECNET/H Interface Board software package (SW0DNC-MNETH-B)

CC-Link System Master/Local Interface Board software package (SW1DNC-CCBD2-B)

CC-Link IE Field Network Interface Board software package (SW1DNC-CCIEF-J/-B)

CC-Link IE Controller Network Interface Board software package (SW1DNC-MNETG-B)

C Controller Interface Module utility (SW1DNC-QSCCF-B)

MELSOFT EM Software Development Kit (SW1DND-EMSDK-B)

Revised the description regarding “Countermeasures for Customers”.

Added a "Countermeasures for Products" section and listed the products that have been fixed.