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

Release date: May 14, 2024
Last update date: January 30,2025
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	All versions
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	All versions
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)	All versions
MR Configurator (SETUP221)	All versions
MR Configurator2	"1.150G" and prior
Position Board Utility2(MRZJW3-MC2-UTL)	All versions
MX Component	"5.007H" and prior
MX OPC Server DA/UA (Software packaged with MC Works64)	All versions
PX Developer/Monitor Tool	All versions
RT ToolBox3	"2.20W" and prior
RT VisualBox	All versions

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

Setting/monitoring tools for the C Controller module (SW4PVC-CCPU)	All versions
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)	All versions
MELSOFT EM Software Development Kit (SW1DND-EMSDK-B)	All versions

(*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)

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

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
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
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
MR Configurator2	"1.155M" or later
MX Component	"5.008J" or later
RT ToolBox3	"2.50C" 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

Mitigations / Workarounds

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 an 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

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.