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

Release date: May 14, 2024
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	All versions
CSGL (GX Works2 connection configuration)	All versions
CW Configurator	All versions
Data Transfer	All versions
Data Transfer Classic	All versions
EZSocket (*1)	All versions
FR Configurator SW3	All versions
FR Configurator2	All versions
GENESIS64	All versions
GT Designer3 Version1 (GOT1000)	All versions
GT Designer3 Version1 (GOT2000)	All versions
GT SoftGOT1000 Version3	All versions
GT SoftGOT2000 Version1	All versions
GX Developer	All versions
GX LogViewer	All versions
GX Works2	All versions
GX Works3	All versions
iQ Works (MELSOFT Navigator)	All versions
MI Configurator	All versions
Mitsubishi Electric Numerical Control Device Communication Software (FCSB1224)	All versions
MR Configurator (SETUP221)	All versions
MR Configurator2	All versions
MRZJW3-MC2-UTL	All versions
MX Component	All versions
MX OPC Server DA/UA (Software packaged with MC Works64)	All versions
PX Developer/Monitor Tool	All versions
RT ToolBox3	All versions
RT VisualBox	All versions
Setting/monitoring tools for the C Controller module (SW4PVC-CCPU)	All versions

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

SW0DNC-MNETH-B	All versions
SW1DNC-CCBD2-B	All versions
SW1DNC-CCIEF-J / -B	All versions
SW1DNC-MNETG-B	All versions
SW1DNC-QSCCF-B	All versions
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.

Countermeasures for Customers

Customers using the affected products should take the following mitigations/workarounds.

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.

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

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