Denial-of-Service (DoS) Vulnerability and Arbitrary Command Execution Vulnerability due to OpenSSL Vulnerabilities in Multiple FA Products

Release date: August 2, 2022
Last update date: January 31, 2023
Mitsubishi Electric Corporation

■Overview

Denial-of-service(DoS) vulnerability and arbitrary command execution vulnerability due to OpenSSL vulnerabilities exist in multiple Mitsubishi Electric FA Products. An attacker could cause denial-of-service (DoS) condition or execute arbitrary malicious commands by sending a specially crafted packet. (CVE-2022-0778, CVE-2022-1292)

■CVSS

CVE-2022-0778 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H Base Score:7.5
CVE-2022-1292 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H Base Score:9.8

■Affected products

Affected products and versions are below.

No.	Product Name	Model Name	Affected software/firmware version	Applicable CVE ID
1	GOT2000 compatible HMI software	GT SoftGOT2000	1.275M	CVE-2022-0778 CVE-2022-1292
2	CC-Link IE TSN Industrial Managed Switch	NZ2MHG-TSNT8F2 NZ2MHG-TSNT4	"03" and prior	CVE-2022-0778
3	MELSEC iQ-R Series OPC UA Server Module	RD81OPC96	"08" and prior	CVE-2022-0778

[How to check the version in use]

1. GOT2000 compatible HMI software (Model Name: GT SoftGOT2000)
   (1) Run GT SoftGOT2000.
   (2) From the Help menu, select [About GT SoftGOT2000...].
   (3) Check the version on "About GT SoftGOT2000" window (see Figure 1).

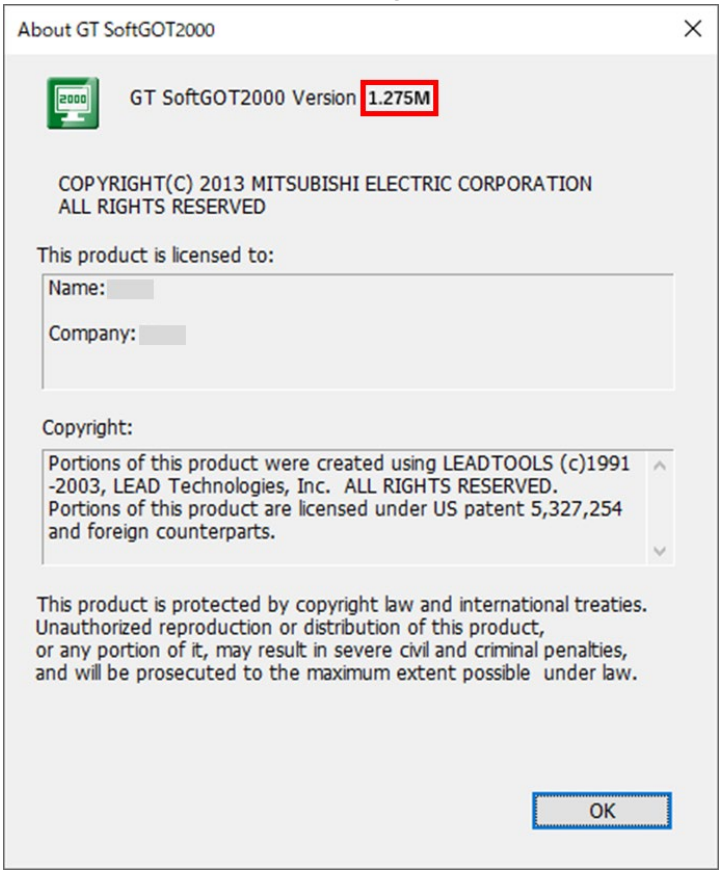

Figure 1 GT SoftGOT2000 version information view

2. CC-Link IE TSN Industrial Managed Switch (Model Name: NZ2MHG-TSNT8F2, NZ2MHG-TSNT4)
(1) After you log into NZ2MHG-TSNT8F2 or NZ2MHG-TSNT4 with the web interface, [Device Summary] screen is displayed.
(2) Confirm the first 2 digits of Firmware Version on Model Information displayed in [Device Summary] screen.(see Figure 2)
ex) When "02 Build xxxx" is displayed, its firmware version is "02".

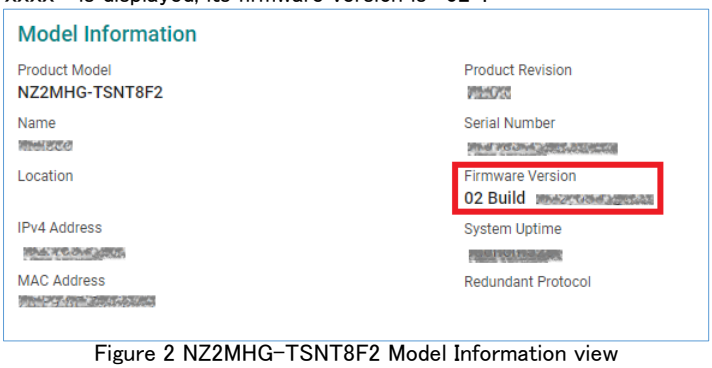

Figure 2 NZ2MHG-TSNT8F2 Model Information view

3. MELSEC iQ-R Series OPC UA Server Module (Model Name: RD81OPC96)
(1) Run engineering software(GX Works3, CW Configurator) and connect to PLC.
(2) Select [Diagnostics] -> [System Monitor] -> [Product Information List].
(3) [Product Information List] will be displayed and confirm the Firmware Version.(see Figure 3).

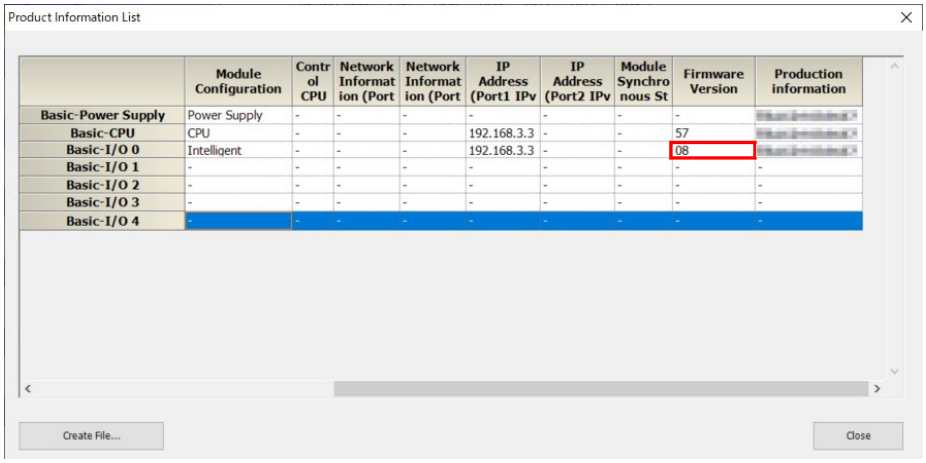

Figure 3 Engineering Software Product Information List view

■Description

Denial-of-service(DoS) vulnerability (CVE-2022-0778) and arbitrary command execution vulnerability (CVE-2022-1292) exist in multiple Mitsubishi Electric FA Products due to the following vulnerabilities in OpenSSL.

・CVE-2022-0778: Loop with Unreachable Exit Condition ('Infinite Loop') (CWE-835)
・CVE-2022-1292: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') (CWE-78)

■Impact

The vulnerabilities could allow an attacker to cause a denial-of-service (DoS) condition or execute arbitrary malicious commands by sending specially crafted packets.

■Countermeasures

Please update to the fixed versions by following the steps below.

[Fixed versions]

No.	Product Name	Model Name	Fixed software/firmware version
1	GOT2000 compatible HMI software	GT SoftGOT2000	1.280S or later
2	CC-Link IE TSN Industrial Managed Switch	NZ2MHG-TSNT8F2 NZ2MHG-TSNT4	"04" or later
3	MELSEC iQ-R Series OPC UA Server Module	RD81OPC96	"09" or later

[Update steps]

1. GOT2000 compatible HMI software (Model Name: GT SoftGOT2000)
   (1) Please contact your local Mitsubishi Electric representative to obtain the fixed version of GT SoftGOT2000 and install it on a personal computer. For detailed installation procedures, please refer to "GT SoftGOT2000 Version1 Operation Manual (SH-081201ENG)".
   (2) Refer to the <How to check the version in use> to check that the software has been updated to the fixed versions.

2. CC-Link IE TSN Industrial Managed Switch (Model Name: NZ2MHG-TSNT8F2, NZ2MHG-TSNT4)
   (1) Please contact your local Mitsubishi Electric representative to obtain the fixed firmware version of CC-Link IE TSN Industrial Managed Switch.
   (2) After you log into NZ2MHG-TSNT8F2 or NZ2MHG-TSNT4 with the web interface, please update the firmware to the above mentioned fixed firmware version file by the function of [System] -> [System Management] -> [Firmware Upgrade] from Function menu.
   For the detailed procedures, please refer to "CC-Link IE TSN Industrial Managed Switch User's Manual (SH-082449ENG)".
   (3) Refer to the <How to check the version in use> to check that the firmware has been updated to the fixed version.

3. MELSEC iQ-R series OPC UA Server Module (Model Name: RD81OPC96)
   (1) Please contact your local Mitsubishi Electric representative to obtain the fixed firmware version of OPC UA Server Module.
   (2) Please update the firmware of OPC UA Server Module using an SD memory card.
   For the detailed procedures, please refer to "MELSEC iQ-R Module Configuration Manual (SH-081262ENG)".
   (3) Refer to the <How to check the version in use> to check that the firmware has been updated to the fixed version.

■Mitigations

Mitsubishi Electric recommends that customers take the following mitigations to minimize the risk of exploiting these vulnerabilities:

・When Internet access is required, use a virtual private network (VPN) or other means to prevent unauthorized access.
・Use the products within a LAN and block access from untrusted networks and hosts.
・Restrict physical access to your computer with the products installed and network equipment on the same network.

Also, recommends to take the following mitigations according to the affected products.

1. GOT2000 compatible HMI software (Model Name: GT SoftGOT2000)
   ・Update the OPC UA server to the latest version.
   ・Install antivirus software on your computer with the products installed.

2. CC-Link IE TSN Industrial Managed Switch (Model Name: NZ2MHG-TSNT8F2, NZ2MHG-TSNT4)
   ・After you log into NZ2MHG-TSNT8F2 or NZ2MHG-TSNT4 with the web interface, change user name and password from default setting at [Account Management] displayed on the function menu. Also, set the proper access permissions depending on the users.

3. MELSEC iQ-R Series OPC UA Server Module (Model Name: RD81OPC96)
   ・Update the OPC UA Client to latest version.
   ・Use legitimate certificate(certificate that can be determined not to be fabricated) on OPC UA Client side.

■Contact information

Please contact your local Mitsubishi Electric representative.

< Inquiries | MITSUBISHI ELECTRIC FA >
https://www.mitsubishielectric.com/fa/support/index.html

■Update history

January 31, 2023

Added the fixed firmware version and update steps of RD81OPC96 to “Countermeasures”.

November 1, 2022

Added the fixed firmware version and update steps of NZ2MHG-TSNT8F2 and NZ2MHG-TSNT4 to “Countermeasures”.

August 30, 2022

Added NZ2MHG-TSNT4 to “Affected products”, “Countermeasures” and “Mitigations”.

August 18, 2022

Added NZ2MHG-TSNT8F2 and RD81OPC96 to “Affected products”, “Countermeasures” and “Mitigations”.