Multiple Denial-of-Service Vulnerabilities in Multiple FA Engineering Software

Release date: December 16, 2021
Last update date: July 28, 2022
Mitsubishi Electric Corporation

■Overview

Multiple Denial-of-Service (DoS) vulnerabilities exist in multiple Mitsubishi Electric FA engineering software. If the software opens a malicious project file (*1) specially crafted by an attacker, they may result in DoS condition. (CVE-2021-20606, CVE-2021-20607)

The product names and versions affected by vulnerabilities are listed below.

(*1) Data file created by the software

■CVSS

CVE-2021-20606: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H Base Score:5.5
CVE-2021-20607: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H Base Score:5.5

■Affected products

<Products and Versions>
GX Works2, versions 1.606G and prior
MELSOFT Navigator, versions 2.84N and prior
EZSocket, versions 5.4 and prior (*2)

<How to Check the Versions>
GX Works2: Refer to "3.4.4 Checking version of GX Works2" in "GX Works2 Version 1 Operating Manual (Common)".
MELSOFT Navigator: Refer to "8.3 Check Version Information of MELSOFT Navigator" in "MELSOFT Navigator Version2 Help".

(*2) EZSocket is a communication middleware for Mitsubishi Electric partner companies. Mitsubishi Electric will inform the partner company directly how to check the version.

■Description

Multiple Denial-of-Service (DoS) vulnerabilities below exist in multiple Mitsubishi Electric FA engineering software.

CVE-2021-20606: Out-of-bounds Read (CWE-125)
CVE-2021-20607: Integer Underflow (CWE-191)

■Impact

If the software opens a malicious project file specially crafted by an attacker, they may result in DoS condition.

■Countermeasures

The fixed software and versions are as follows:

<Products and Versions>
GX Works2, version 1.610L or later
MELSOFT Navigator, version 2.86Q or later
EZSocket, version 5.5 or later (*3)

<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" located in the folder unzipped and install it.

(*3) Mitsubishi Electric will directly provide the fixed version of EZSocket to the partner companies.

■Mitigations

For customers who use the software for which the fixed version has not been released or who are not able to immediately update the software, Mitsubishi Electric recommends to take the following mitigation measures to minimize the risk of being exploited these vulnerabilities:

-Make sure that malicious attackers cannot access project files that are stored in your computer/server via untrusted network or host.
-Install an antivirus software in your personal computer running the software.
-Don't open the project files, such as attached to e-mail that was sent from an untrusted sender.
-Please execute procedures below for GX Works2 project files read from PLC via "Batch Read" function of MELSOFT Navigator or EZSocket.

1. With GX Works2 1.610L or later, open the project file that is read from PLC via "Batch Read" function of MELSOFT Navigator or EZSocket.
2. Enable the option [Enable the security check for the project] ([Options] -> [Project] -> [Common Setting]) and save the project.

■Contact information

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

■Update history

July 28, 2022
Added fixed product as below.
EZSocket

June 30, 2022
Added fixed product as below.
MELSOFT Navigator