Denial-of-Service (DoS) Vulnerability in GX Works2

Release date: December 16, 2021
Mitsubishi Electric Corporation

■Overview

Denial-of-Service (DoS) vulnerability exists in Mitsubishi Electric's FA engineering software GX Works2. If a malicious attacker tampers with a program file in a Mitsubishi Electric PLC by sending malicious crafted packets to the PLC, reading the program file into GX Works2 may result in a denial of service (DoS) condition in GX Works2. (CVE-2021-20608)

■CVSS

CVE-2021-20608: CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:H Base Score:5.3

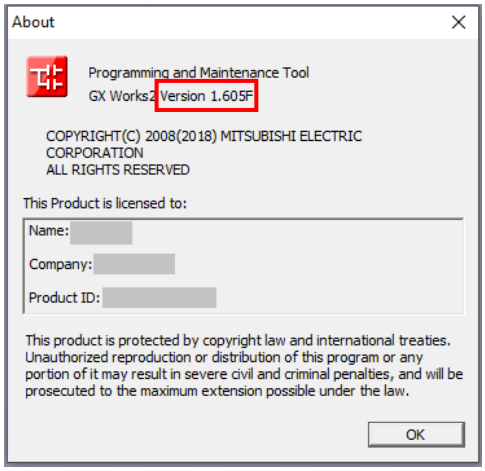
■Affected products

<Products and Versions>

GX Works2, versions 1.606G and prior

<How to Check the Versions>

1. Run GX Works2.
2. Select [Help] -> [About].
3. Check version by [About GX Works2] screen.



■Description

Denial-of-Service (DoS) vulnerability due to Improper Handling of Length Parameter Inconsistency (CWE-130) exists in Mitsubishi Electric's FA engineering software GX Works2.

■Impact

If a malicious attacker tampers with a program file in a Mitsubishi Electric PLC by sending malicious crafted packets to the PLC, reading the program file into GX Works2 may result in a denial of service (DoS) condition in GX Works2.
This vulnerability does not cause PLC malfunction.

■Countermeasures

Download fixed Ver. 1.610L or later 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. Please run "setup.exe" in the extracted folder to install.

■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 this vulnerability:

-Restrict the connection of all control system devices and systems to the network so that they can only be accessed from trusted networks and hosts.
-Locate control system networks and remote devices behind firewalls and isolate them from the business network.
-Use Virtual Private Network (VPN) when remote access to Mitsubishi Electric PLC is required.

■Contact information

Please contact your local Mitsubishi Electric representative.

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