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

Release date August 2, 2022
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.

Product	Affected software version
GT SoftGOT2000	1.275M

[How to check the version in use]

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).

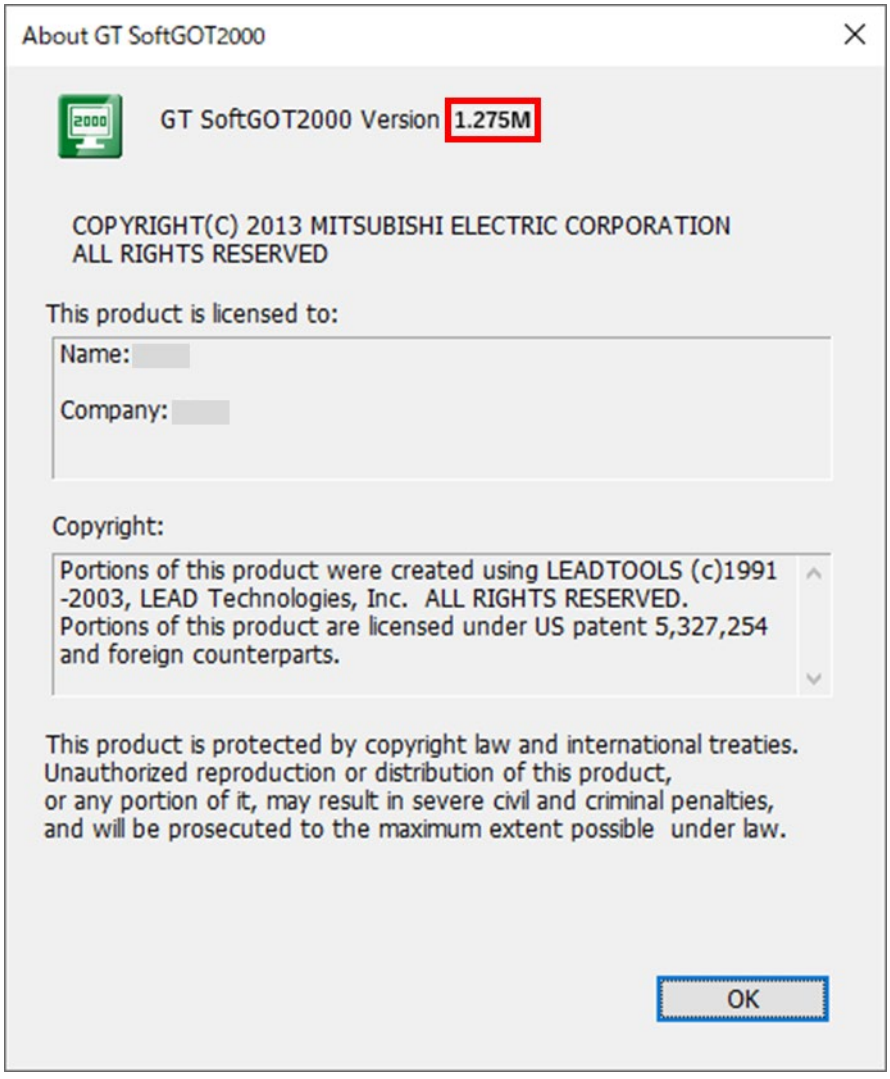

Figure 1 GT SoftGOT2000 version information view

■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]

Product	Fixed software version
GT SoftGOT2000	1.280S or later

[Update steps]

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.

■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.
・Update the OPC UA server to the latest version.
・Install antivirus software on your computer with the products installed.
・Restrict physical access to your computer with the products installed and network equipment on the same network.

■Contact information

Please contact your local Mitsubishi Electric representative.

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