Information Disclosure and Denial-of-Service (DoS) Vulnerabilities due to OpenSSL vulnerabilities on MELSOFT GT OPC UA Client

Release date May 10, 2022
Mitsubishi Electric Corporation

■Overview

Information disclosure and denial-of-service (DoS) vulnerabilities due to out-of-bounds read and integer overflow (Roundup) in OpenSSL exist in the MELSOFT GT OPC UA Client. This product works in conjunction with the GT SoftGOT2000 to provide the GT SoftGOT2000 with a communication function with OPC UA servers. A remote malicious attacker could exploit these vulnerabilities in any way, such as by sending a specially crafted message, to disclose information on memory in GT SoftGOT2000 or to cause denial of service (DoS) condition on it. (CVE-2021-3712, CVE-2021-23840)

■CVSS

CVE-2021-3712 CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:H Base Score:7.4
CVE-2021-23840 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H Base Score:7.5

■Affected products

The following products and versions combinations with "OPC UA Client Connections" are affected.

[Products and Versions]

Affected products and versions are below.

Product	Software version
MELSOFT GT OPC UA Client	1.00A – 1.02C

[Product and version to be combined]

The products and versions to be combined are below.

Product	Software version
GT SoftGOT2000	1.215Z – 1.270G

[How to check the version in use]

For MELSOFT GT OPC UA Client

1. Run the MELSOFT GT OPC UA Client.
2. From the Help menu, select [About GT OPC Client Setting Tool...].
3. Check the version on "About GT OPC UA Client Setting Tool" window (see Figure 1).

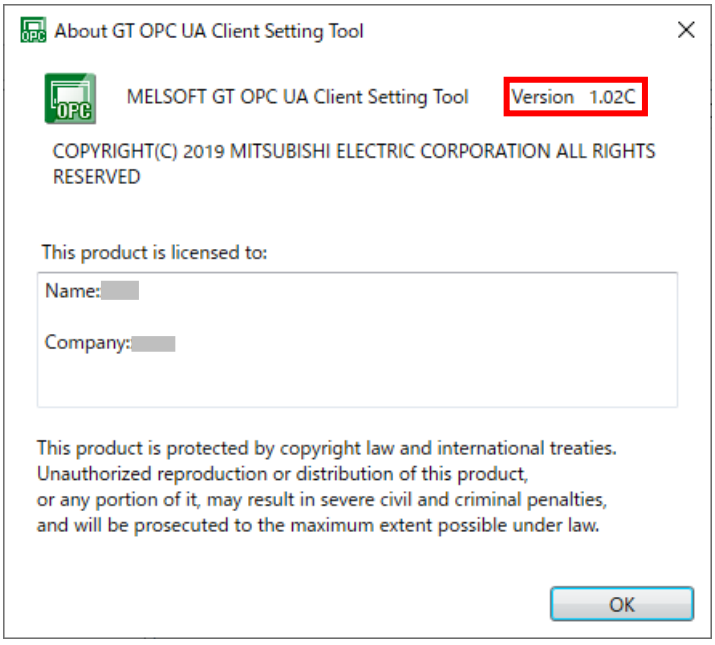

Figure 1 MELSOFT GT OPC UA Client

For GT SoftGOT2000

1. Run the GT SoftGOT2000.
2. From the Help menu, select [About GT SoftGOT2000...].
3. Check the version on "About GT SoftGOT2000" window (see Figure 2).

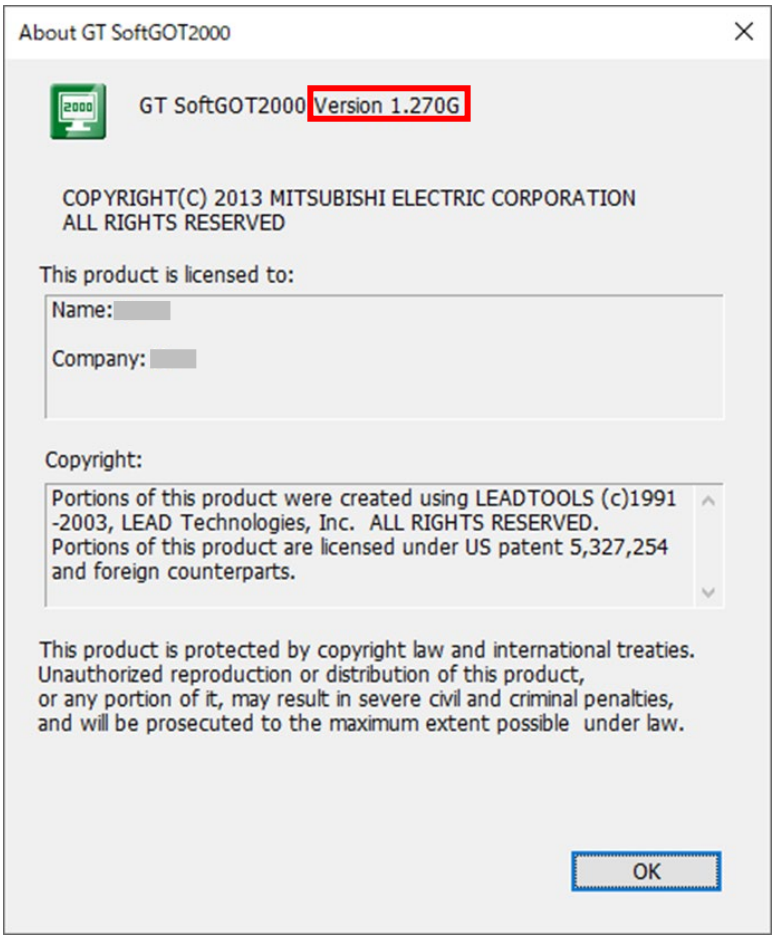

Figure 2 GT SoftGOT2000

■Description

Information disclosure and denial-of-service (DoS) vulnerabilities due to out-of-bounds read and integer overflow (Roundup) in OpenSSL exist in the MELSOFT GT OPC UA Client.

・CVE-2021-3712: Out-of-bounds read (CWE-125)
・CVE-2021-23840 Integer overflow or wraparound (CWE-190)

■Impact

A remote malicious attacker could exploit these vulnerabilities in any way, such as by sending a specially crafted message, to disclose information on memory in GT SoftGOT2000 or to cause denial of service (DoS) condition on it.

■Countermeasures

Please update to the fixed versions by following the steps below. In addition, update the GT SoftGOT2000 to 1.275M or later in accordance with the MELSOFT GT OPC UA Client update.

[Fixed version]

Product	Software version
MELSOFT GT OPC UA Client	1.03D or later

[Update steps]

For MELSOFT GT OPC UA Client

1. Obtain the fixed version of MELSOFT GT OPC UA Client and install into the PC.
   Please contact your local representative about MELSOFT GT OPC UA Client.
2. Refer to the <How to check the versions in use> to check that the software has been updated to the fixed versions.

For GT SoftGOT2000

1. Obtain the fixed version of the GT SoftGOT2000 and install into the PC.
   Please contact your local representative about the GT SoftGOT2000.
2. Refer to the <How to check the versions 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 connecting the products to the Internet, use a virtual private network (VPN), etc. to prevent spoofing and sniffing.
・Use the products within the 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 product installed.
・Restrict physical access to your computer with the product installed and network equipment on the same network.

■Contact information

For inquiries about products, please contact your local Mitsubishi Electric representative.
< Inquiries | MITSUBISHI ELECTRIC FA >
https://www.mitsubishielectric.com/fa/support/index.html