# Arbitrary Command Execution Vulnerability
# due to OpenSSL Vulnerability in GT SoftGOT2000

Release date: November 15, 2022
Mitsubishi Electric Corporation

## ■Overview

Arbitrary command execution vulnerability due to OpenSSL vulnerability exists in GT SoftGOT2000. An attacker could execute malicious OS commands by sending a specially crafted certificate. (CVE-2022-2068)

## ■CVSS

CVE-2022-2068 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H Base Score:9.8

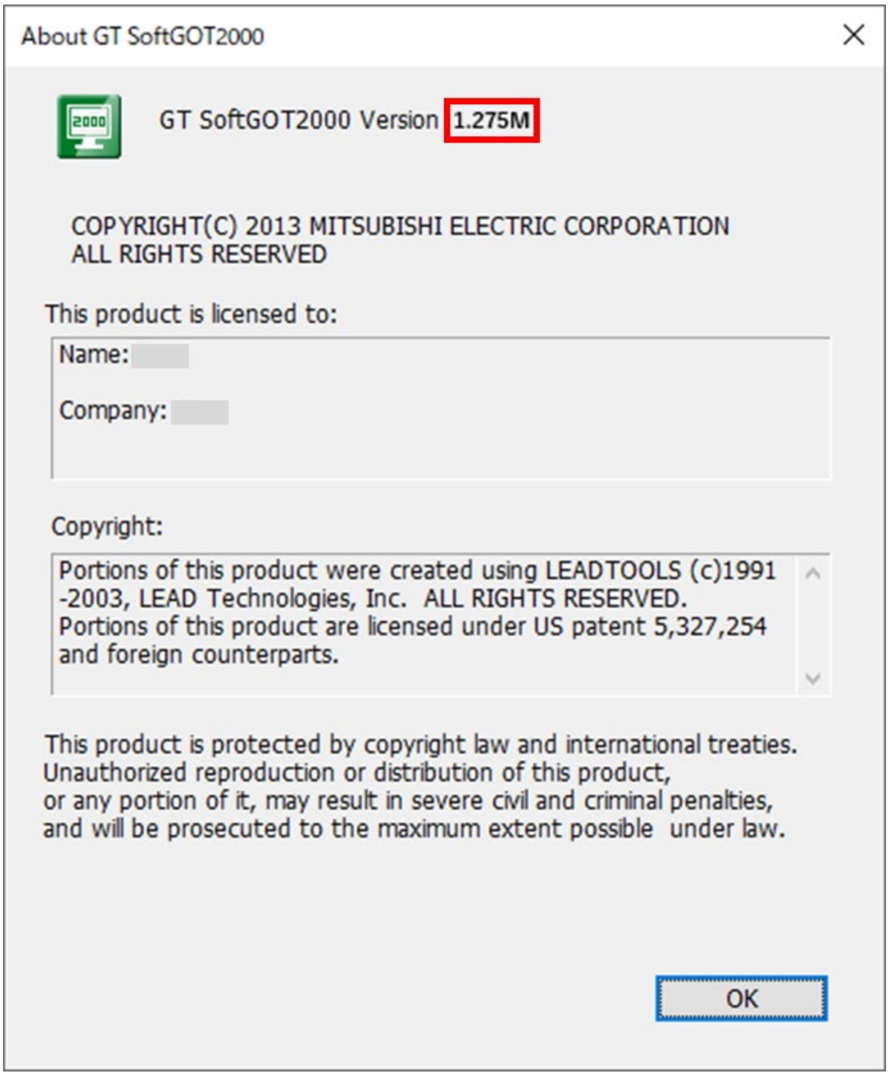
## ■Affected products

Affected products and versions are below.

| Product | Affected software version |
|---|---|
| GT SoftGOT2000 | 1.275M – 1.280S |

[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).



About GT SoftGOT2000

GT SoftGOT2000 Version 1.275M

COPYRIGHT(C) 2013 MITSUBISHI ELECTRIC CORPORATION
ALL RIGHTS RESERVED

This product is licensed to:

Name:

Company:

Copyright:

Portions of this product were created using LEADTOOLS (c)1991-2003, LEAD Technologies, Inc. ALL RIGHTS RESERVED.
Portions of this product are licensed under US patent 5,327,254 and foreign counterparts.

This product is protected by copyright law and international treaties.
Unauthorized reproduction or distribution of this product,
or any portion of it, may result in severe civil and criminal penalties,
and will be prosecuted to the maximum extent possible under law.

Figure 1 GT SoftGOT2000 version information view

## ■Description

Malicious OS command execution vulnerability (CVE-2022-2068) exists in GT SoftGOT2000 due to the following issue in OpenSSL.

・CVE-2022-2068: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') (CWE-78)

## ■Impact

The vulnerability could allow an attacker to execute malicious OS commands by sending specially crafted certificate.

## ■Countermeasures

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

[Fixed versions]

| Product | Fixed software version |
|---|---|
| GT SoftGOT2000 | 1.285X or later |

[Update steps]

1. Please contact your local Mitsubishi Electric representative to obtain the fixed version of GT SoftGOT2000 and install it on your 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 this vulnerability:

・Use the products within a LAN and block access from untrusted networks and hosts.
・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.
・Do not store untrusted certificates.
・Do not click on web links contained in e-mails or other communications from untrusted sources.

## ■Contact information

Please contact your local Mitsubishi Electric representative.

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