Leading users to unintended operation Vulnerability and Information Disclosure and Spoofing Vulnerability in GOT Mobile Function on GOT2000 Series and GT SoftGOT2000

Release date: February 2, 2023
Mitsubishi Electric Corporation

■Overview

Leading users to unintended operation vulnerability and information disclosure and spoofing vulnerability exist in GOT Mobile function on GOT2000 Series and GT SoftGOT2000. Attackers can induce users to perform unintended operations through clickjacking (an attack that induces users into clicking a webpage element which is invisible or disguised as another element) (CVE-2022-40268) or disclose sensitive information from users' browsers or impersonate legitimate users by abusing inappropriate HTML attributes (CVE-2022-40269).

■CVSS[1]

CVE-2022-40268	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:N/I:H/A:N	Base Score:6.1
CVE-2022-40269	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N	Base Score:6.8

■Affected products

Affected products and versions are listed below.

Affected when using the "GOT Mobile" function

Series	Model	Affected GOT Mobile versions
GOT2000 Series	GT27 model	01.14.000 - 01.47.000
	GT25 model	01.14.000 - 01.47.000

Affected when using the "GOT Mobile" function

Series	Model	Affected software versions
GT SoftGOT2000	-	1.265B - 1.285X

<How to check the versions in use>

For how to check the versions in use, please refer to the following manual. The latest version of manual is available from MITSUBISHI ELECTRIC FA Global Website (https://www.mitsubishielectric.com/fa).

[For GT27/GT25 models]
GOT2000 Series User's Manual (Utility) (SH-081195ENG)
"6.9 Package Data Management" - "Property operation"

[For GT SoftGOT2000]
GT SoftGOT2000 Version1 Operating Manual (SH-081201ENG)
"2.7 Help" - "Confirming GT SoftGOT2000 version (When [About GT SoftGOT2000...] is selected)"

■Description

Leading users to unintended operation vulnerability (CVE-2022-40268) due to Improper Restriction of Rendered UI Layers or Frames (CWE-1021)[2] and information disclosure and spoofing (Authentication Bypass by Spoofing (CWE-290)[3]) vulnerability (CVE-2022-40269) exist in the GOT Mobile function of the GOT2000 Series and GT SoftGT2000.

■Impact

The vulnerabilities could allow an attacker to leading legitimate users to unintended operation through clickjacking (CVE-2022-40268) and disclose sensitive information from users' browsers or impersonate legitimate users by abusing inappropriate HTML attributes (CVE-2022-40269).

[1] https://www.first.org/cvss/v3.1/specification-document

[2] https://cwe.mitre.org/data/definitions/1021.html

[3] https://cwe.mitre.org/data/definitions/290.html

■Countermeasures

In the case of using the affected products and versions, please update to the fixed versions by following the steps below.

<Fixed versions>

We have fixed the vulnerabilities at the following versions.

(GT Designer3 Version1 (GOT2000) Ver.1.290C or later)

Series	Model	Fixed GOT Mobile versions
GOT2000 Series	GT27 model	01.48.000 or later
	GT25 model	01.48.000 or later

Series	Model	Fixed software versions
GT SoftGOT2000	–	1.290C or later

<Update steps>

[For GT27/GT25 models]

1. Download the fixed version of GT Designer3 Version1 (GOT2000) and install on a personal computer.
   Please contact your local Mitsubishi Electric representative for GT Designer3 Version1 (GOT2000).
2. Start the GT Designer3 Version1 (GOT2000) and open the project data used in affected products.
3. Select [Write to GOT] from [Communication] menu to write the required package data to the GOT.
   Please refer to the GT Designer3 Version1 (GOT2000) Screen Design Manual (SH-081220ENG).
   "4. COMMUNICATING WITH GOT"
4. After writing the required package data to the GOT, refer to the <How to check the versions in use> and check that the software has been updated to the fixed versions.

[For GT SoftGOT2000]

1. Download the fixed version of GT SoftGOT2000 Version1 from the following site and install on a personal computer.
   Please contact your local Mitsubishi Electric representative about GT SoftGOT2000 Version1.
2. Refer to the <How to check the versions in use> and check that the software has been updated to the fixed versions.

■Mitigations/Workarounds

Mitsubishi Electric recommends that customers take the following mitigations to minimize the risk of exploiting these vulnerabilities:

[Mitigations]

・When Internet access is required, use a firewall, virtual private network (VPN), etc. to prevent unauthorized access.
・Use the products within a LAN and block access from untrusted networks and hosts.
・Install antivirus software on your computer with the products installed.
・Use the IP filter function*1 to restrict the accessible IP addresses.

*1: GT Designer3 (GOT2000) Screen Design Manual (SH-081220ENG). "5.4.3 Setting the IP filter"

[Workarounds]

・Disable GOT Mobile Function.

■Contact information

Please contact your local Mitsubishi Electric representative.

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