Denial-of-Service Vulnerability in TCP/IP Stack of GOT and Tension Controller

Release date: December 3, 2020
Last update date: January 20, 2022
Mitsubishi Electric Corporation

■Overview

There is a Denial of Service (DoS) vulnerability in GT21 model of GOT2000 series, GS21 model of GOT SIMPLE series and Tension Controller due to an out-of-bounds read. Affected products allow malicious attackers to cause deterioration of communication performance or cause a DoS condition of the TCP communication functions of the products by sending specially crafted packets. (CVE-2020-5675)

■CVSS

CVE-2020-5675 CVSS: 3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H Base Score:7.5

■Affected products

Affected products and versions are below.

(1) Human-Machine Interfaces-GOT

Series	Model	Product Name	Affected Basic System Application versions
GOT2000 series	GT21 model	GT2107-WTBD	V01.39.000 and earlier
		GT2107-WTSD	V01.39.000 and earlier
		GT2104-RTBD	V01.39.000 and earlier
		GT2104-PMBD	V01.39.000 and earlier
		GT2103-PMBD	V01.39.000 and earlier
GOT SIMPLE series	GS21 model	GS2110-WTBD	V01.39.000 and earlier
		GS2107-WTBD	V01.39.000 and earlier
		GS2110-WTBD-N	V01.39.000 and earlier
		GS2107-WTBD-N	V01.39.000 and earlier

<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).

GOT2000 Series User's Manual (Utility) (SH-081195ENG)
"15.2 OS information"

(2) Tension Controller

Model	Name of screen package data	Affected screen package data version
LE7-40GU-L	LE7-40GU-L Screen package data for CC-Link IEF Basic	V1.00
	LE7-40GU-L Screen package data for MODBUS/TCP	V1.00
	LE7-40GU-L Screen package data for SLMP	V1.00

<How to check the versions in use>

Check the screen package data version on the tension controller screen "Screen number 961: The Main unit ROM/Screen version".

Refer to the following manual for how to display and operate the above screen. Contact your local Mitsubishi Electric representative for the latest manual.

LE7-40GU-L APPLICATION MANUAL (SH-170022ENG)

■Description

There is a Denial of Service (DoS) vulnerability in GT21 model of GOT2000 series, GS21 model of GOT SIMPLE series and Tension Controller due to an out-of-bounds read (CWE-125).

■Impact

Affected products allow malicious attackers to cause deterioration of communication performance or cause a DoS condition of the TCP communication functions of the products by sending specially crafted packets. Turn off and on the GOT or Tension Controller to recover the DoS condition.

■Countermeasures

(1) Human-Machine Interfaces-GOT

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 vulnerability at the following versions.

Fixed Basic System Application is shipped with GT Designer3(2000) versions 1.255R or later.

Series	Model	Product Name	Fixed Basic System Application versions
GOT2000 series	GT21 model	GT2107-WTBD	V01.40.000 or later
		GT2107-WTSD	V01.40.000 or later
		GT2104-RTBD	V01.40.000 or later
		GT2104-PMBD	V01.40.000 or later
		GT2103-PMBD	V01.40.000 or later
GOT SIMPLE series	GS21 model	GS2110-WTBD	V01.40.000 or later
		GS2107-WTBD	V01.40.000 or later
		GS2110-WTBD-N	V01.40.000 or later
		GS2107-WTBD-N	V01.40.000 or later

<Update procedure>

① Download the fixed version of MELSOFT GT Designer3(2000) and install into the PC.
Please contact your local representative about MELSOFT GT Designer3(2000).

② Start the MELSOFT GT Designer3(2000) 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 (GOT2000) Screen Design Manual.
″4. COMMUNICATING WITH GOT″

④ After write the required package data to the GOT, refer to the【How to check the versions in use】and check the fixed versions.

(2) Tension Controller

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 vulnerability in the following versions.

Model	Name of screen package data	Fixed screen package data versions
LE7-40GU-L	LE7-40GU-L Screen package data for CC-Link IEF Basic	V1.01 or later
	LE7-40GU-L Screen package data for MODBUS/TCP	V1.01 or later
	LE7-40GU-L Screen package data for SLMP	V1.01 or later

<Update procedure>

① Contact your local Mitsubishi Electric representative for the fixed version of the screen package data.

② Install the engineering tool (“Data Transfer Tool” or “GT Designer 3 (GOT2000)”) in your PC.
Contact your local Mitsubishi Electric representative for the latest engineering tool.

③ Connect LE7-40GU-L and your PC with a USB cable.

④ Write the screen package data to LE7-40GU-L using the “GOT write” function of the engineering tool.

⑤ After writing is completed, restart LE7-40GU-L.

⑥ Refer to the【How to check the versions in use】and check that it is the fixed versions.

■Mitigations

Please restrict access to the product only from trusted networks and hosts.

■Contact information

Please contact your local Mitsubishi Electric representative.

< Inquiries | MITSUBISHI ELECTRIC FA >

https://www.mitsubishielectric.com/fa/support/index.html

■Update history

January 20, 2022

For Tension Controller, added “How to check the versions in use” to “Affected products and version”.

For Tension Controller, added “Update procedure” and “Fixed Versions” to “Countermeasures”.

May 11, 2021

Added “How to check the versions in use” to “Affected products and version”

Added “Update procedure” and “Fixed Versions” to “Countermeasures”.