Denial-of-Service (DoS) Vulnerability in MODBUS/TCP slave communication function on GOT and Tension Controller

Release date: May 11, 2021
Last update date: January 20, 2022
Mitsubishi Electric Corporation

■Overview

Denial-of-Service (DoS) vulnerability exists in the MODBUS/TCP slave communication function of GOT2000 series, GOT SIMPLE series, SoftGOT2000 and Tension Controller. A malicious attacker can stop the communication function of the products by sending a specially crafted packet. (CVE-2021-20589)

■CVSS

CVE-2021-20589　CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H　Base Score:5.9

■Affected products

Affected products and versions are below.

(1) Human-Machine Interfaces-GOT

Affected when using the "MODBUS/TCP Slave, Gateway" communication driver.

Series	Model	Affected communication driver versions
GOT2000 series	GT27 model	01.19.000 ～ 01.38.000
	GT25 model	01.19.000 ～ 01.38.000
	GT23 model	01.19.000 ～ 01.38.000
	GT21 model	01.21.000 ～ 01.39.000
GOT SIMPLE series	GS21 model	01.21.000 ～ 01.39.000
GT SoftGOT2000	―	1.170C ～ 1.250L

<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/GT23 models
GOT2000 Series User's Manual (Utility) (SH-081195ENG)
"6.9 Package Data Management" - "Property operation"

For GT21 models
GOT2000 Series User's Manual (Utility) (SH-081195ENG)
"15.2 OS information"

For GS21 models
GOT SIMPLE Series User's Manual (JY997D52901)
"15.2 OS information"

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

(2) Tension Controller

Affected when using the screen package data for MODBUS/TCP.

Model	Name of screen package data	Affected screen package data version
LE7-40GU-L	LE7-40GU-L Screen package data for MODBUS/TCP	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

Denial-of-Service (DoS) vulnerability exists in the MODBUS/TCP slave communication function of GOT2000 series, GOT SIMPLE series, SoftGOT2000 and Tension Controller due to buffer access with incorrect length value (CWE-805).

■Impact

A malicious attacker, can stop the communication function of the products by sending a specially crafted packet.
In that case, take the following measures to recover.

(1) Human-Machine Interfaces-GOT

It is necessary to turn on/off the GOT or press the GOT reset switch (reset switch is available only on GT27/25/23 models).

GT SoftGOT2000 needs to be restarted because the software will be forcibly terminated.

(2) Tension Controller

Please turn the power of Tension Controller back on.

■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.
(GT Designer3 Version1(GOT2000） Ver.1.255R or later)

Series	Model	Fixed communication driver versions
GOT2000 series	GT27 model	01.39.000 or later
	GT25 model	01.39.000 or later
	GT23 model	01.39.000 or later
	GT21 model	01.40.000 or later
GOT SIMPLE series	GS21 model	01.40.000 or later
GT SoftGOT2000	—	1.255R or later

<Update procedure>

For GOT2000/GOT SIMPLE series

① Download the fixed version of MELSOFT GT Designer3（2000） and install into the PC.
Please contact your local Mitsubishi Electric 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 (SH-081220ENG).
“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.

For GT SoftGOT2000

① Download the fixed version of GT SoftGOT2000 Version1 from the following site and install into the PC.
Please contact your local Mitsubishi Electric representative about GT SoftGOT2000 Version1.

② 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 MODBUS/TCP	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

(1) When connecting the product to the Internet, use a firewall or virtual private network (VPN) to prevent unauthorized access.
(2) Use it within the LAN and make it inaccessible from untrusted networks and hosts.
(3) Install antivirus software on a computer that can access the product.

■Acknowledgement

Mitsubishi Electric would like to thank Parul Sindhwad and Dr. Faruk Kazi of COE–CNDS Lab, VJTI, Mumbai , India.

■Contact information

Please contact your local Mitsubishi Electric representative.

< Inquiries | MITSUBISHI ELECTRIC FA >

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

■Trademarks

■Update history

January 20, 2022

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