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

Release date: July 27, 2021
Mitsubishi Electric Corporation

■Overview

Denial-of-Service (DoS) vulnerability exists in the MODBUS/TCP slave communication function of GOT2000 series and GT SoftGOT2000. A malicious attacker can stop the communication function of the products by rapidly and repeatedly connecting and disconnecting to and from the MODBUS/TCP communication port on GOT. (CVE-2021-20592)

■CVSS

CVE-2021-20592　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 listed below.

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

Series	Model	Affected communication driver versions
GOT2000 series	GT27 model	01.19.000 ～ 01.39.010
	GT25 model	01.19.000 ～ 01.39.010
	GT23 model	01.19.000 ～ 01.39.010

Affected when configuring to use the ″MODBUS/TCP Slave″ communication.

Series	Model	Affected software versions
GT SoftGOT2000	-	1.170C ～ 1.256S

<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 GOT2000 series

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

Denial-of-Service (DoS) vulnerability exists in the MODBUS/TCP slave communication function of GOT2000 series and GT SoftGOT2000 due to missing synchronization (CWE-820).

■Impact

A malicious attacker, can stop the communication function of the products by rapidly and repeatedly connecting and disconnecting to and from the MODBUS/TCP communication port on GOT.

In that case, take the following measures to recover.

For the GOT2000 series, please restart by turning off and on the GOT or pressing the GOT reset switch.

For GT SoftGOT2000, please restart the software since it will be forcibly terminated.

■Countermeasures

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

<Fixed versions>

The fixed versions for the vulnerability is below.

For GOT2000 series

(Fixed communication driver is included in GT Designer3 Version1(GOT2000) Ver.1.260W or later)

Series	Model	Fixed communication driver versions
GOT2000 series	GT27 model	01.40.000 or later
	GT25 model	01.40.000 or later
	GT23 model	01.40.000 or later

For GT SoftGOT2000

Series	Model	Fixed software versions
GT SoftGOT2000	–	1.260W or later

<Update procedure>

For GOT2000 series

1) Download the fixed version of MELSOFT GT Designer3(2000) and install it on your personal computer.
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 "4. COMMUNICATING WITH GOT" in the GT Designer3 (GOT2000) Screen Design Manual (SH-081220ENG).
4) After writing the required package data to the GOT, refer to the <How to check the versions in use> and check that the driver 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 it on your 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

Mitsubishi Electric recommends that customers take the following mitigations to minimize the risk of exploiting this vulnerability:

(1) When connecting the products to the Internet, use a firewall or virtual private network (VPN), etc. to prevent unauthorized access.
(2) Use the products within the LAN and block access from untrusted networks and hosts.
(3) Install antivirus software on your 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

For inquiries about products, please contact your local Mitsubishi Electric representative.

< Inquiries | MITSUBISHI ELECTRIC FA >

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

■Trademarks

MODBUS is a registered trademark of Schneider Electric SA.