# Multiple Denial of Service (DoS) Vulnerabilities in TCP/IP Protocol Stack of GOT and Tension Controller

Release date: September 6, 2021
Last update date: October 5, 2021
Mitsubishi Electric Corporation

■Overview

Multiple Denial of Service (DoS) vulnerabilities due to improper handling of exceptional conditions and improper input validation exist in TCP/IP protocol stack of GOT and Tension Controller. A remote attacker may cause a DoS condition of GOT and Tension Controller by sending specially crafted packets. (CVE-2021-20602, CVE-2021-20603, CVE-2021-20604, CVE-2021-20605)

■CVSS

CVE-2021-20602 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H Base Score:7.5
CVE-2021-20603 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H Base Score:7.5
CVE-2021-20604 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H Base Score:7.5
CVE-2021-20605 CVSS:3.1/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 | Version |
|---|---|---|---|
| GOT2000 series | GT21 model | GT2107-WTBD | All versions |
| | | GT2107-WTSD | All versions |
| | | GT2104-RTBD | All versions |
| | | GT2104-PMBD | All versions |
| | | GT2103-PMBD | All versions |
| GOT SIMPLE series | GS21 model | GS2110-WTBD | All versions |
| | | GS2107-WTBD | All versions |
| | | GS2110-WTBD-N | All versions |
| | | GS2107-WTBD-N | All versions |

(2) Tension Controller

| Product Name | Version |
|---|---|
| LE7-40GU-L | All versions |

■Description

Multiple DoS vulnerabilities due to improper handling of exceptional conditions and improper input validation exist in TCP/IP protocol stack of GOT and Tension Controller.

- Improper Handling of Exceptional Conditions (CWE-755) CVE-2021-20602
- Improper Input Validation (CWE-20) CVE-2021-20603, CVE-2021-20604, CVE-2021-20605

■Impact

A remote attacker may cause a DoS condition of GOT and Tension Controller by sending specially crafted packets.

■Countermeasures

Please carry out the mitigations/workarounds below. We will release a fixed version in the near future.

■Mitigations/Workarounds

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

- Use a firewall or virtual private network (VPN), etc. to prevent unauthorized access when Internet access is required.
- Use within a LAN and block access from untrusted networks and hosts through firewalls.
- Use the IP filter function*1, 2 to restrict the accessible IP addresses.

*1：GT Designer3 (GOT2000) Screen Design Manual(SH-081220ENG). “5.4.3 Setting the IP filter”
*2：GOT support the IP filter function, Tension Controller does not support it.

■Contact information

Please contact your local Mitsubishi Electric representative.

< Inquiries | MITSUBISHI ELECTRIC FA >

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

■Update history

October 5, 2021

Added information to “Overview”, “CVSS”, “Description” and “Countermeasures”.