

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

Release date: December 3, 2020

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 and version

This issue affects the following products:

(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

(2) Tension Controller

Product Name	Version
LE7-40GU-L	All versions

■ 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 the GOT or Tension Controller power. After that, Turn on the GOT or Tension Controller power is required to recover it.

■ Countermeasures

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

■ Mitigations

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

■ Contact information

Please contact your local Mitsubishi Electric representative.