Information Tampering Vulnerability in GOT2000 series, GOT SIMPLE series and GT SoftGOT2000

Release date: November 16, 2021
Mitsubishi Electric Corporation

■Overview

Information tampering vulnerability exists in GOT2000 series, GOT SIMPLE series and GT SoftGOT2000 due to improper input validation (CWE-20) for device value. An attacker may write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. (CVE-2021-20601)

■CVSS

CVE-2021-20601　CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N　Base Score:7.5

■Affected products

Affected products and versions are listed below.

Series	Model	Version
GOT2000 series	GT27 model	All versions
	GT25 model	All versions
	GT23 model	All versions
	GT21 model	All versions
GOT SIMPLE series	GS21 model	All versions

Series	Model	Software versions
GT SoftGOT2000	-	All versions

■Description

Information tampering vulnerability exists in GOT2000 series, GOT SIMPLE series and GT SoftGOT2000 due to improper input validation (CWE-20).

■Impact

An attacker may write a value that exceeds the configured input range limit by sending a malicious packet to rewrite the device value. As a result, the system operation may be affected, such as malfunction.

As described in the precautions in our manual[*1], the input range setting is valid only when input is performed from the GUI of GOT. This setting does not work effectively for input from external equipment via the network.

*1: GT Designer3 (GOT2000) Screen Design Manual(SH-081220ENG). "8.4.3 Precautions for a numerical display object and a numerical input object"

■Countermeasures

Please implement mitigation measures.

■Mitigations

When it is necessary to protect the GOT and system from unauthorized access from external equipment via the network, please take measures such as installing a firewall as described in [Design Precautions] in our manual[*2].

*2: e.g. GT Designer3 (GOT2000) Screen Design Manual(SH-081220ENG). "Design Precautions"

Concretely, the impact of this vulnerability can be mitigated or prevented by implementing one or a combination of the following measures.

(1) Use a firewall or virtual private network (VPN), etc. to prevent unauthorized access when Internet access is required.
(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 and the system.
(4) Use the IP filter function[*3] to restrict the accessible IP addresses.

*3: GT Designer3 (GOT2000) Screen Design Manual(SH-081220ENG). "5.4.3 Setting the IP filter"

■Acknowledgement

Mitsubishi Electric would like to thank Parul Sindhwad and Dr. Faruk Kazi of COE-CNDS Lab, VJTI, Mumbai, India for reporting this vulnerability and a point for improvement of our products.

■Contact information

Please contact your local Mitsubishi Electric representative.

< Inquiries | MITSUBISHI ELECTRIC FA >

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