Denial-of-Service (DoS) Vulnerability in FTP Server Function on GOT2000 Series

Release date: November 24, 2022
Mitsubishi Electric Corporation

■Overview

Denial-of-Service (DoS) vulnerability exists in the FTP server function of the GOT2000 Series. This vulnerability allows an attacker to cause a denial-of-service (DoS) condition by sending a specially crafted command. (CVE-2022-40266)

■CVSS[1]

CVE-2022-40266 CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H Base Score:5.3

■Affected products

Affected products and versions are below.

Affected when using the "FTP server" function

Series	Model	Product Name	Affected FTP server versions
GOT2000 Series	GT27 model	All	01.39.000 and prior
	GT25 model	All	01.39.000 and prior
	GT23 model	All	01.39.000 and prior

<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).

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

■Description

Denial-of-Service (DoS) vulnerability (CVE-2022-40266) exists in the FTP server function of the GOT2000 Series due to Improper Input Validation (CWE-20)[2].

■Impact

The vulnerability could allow an attacker to cause a denial-of-service (DoS) condition by sending specially crafted command when the attacker has logged into the FTP server (GOT) from any FTP client.

■Countermeasures

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.1.285X or later)

Series	Model	Product Name	Fixed FTP server versions
GOT2000 Series	GT27 model	All	01.47.000 or later
	GT25 model	All	01.47.000 or later
	GT23 model	All	01.47.000 or later

<Update steps>

1. Download the fixed version of GT Designer3 Version1 (GOT2000) and install on a personal computer.
   Please contact your local Mitsubishi Electric representative for GT Designer3 Version1 (GOT2000).
2. Start the GT Designer3 Version1 (GOT2000) 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 Version1 (GOT2000) Screen Design Manual (SH-081220ENG).
   "4. COMMUNICATING WITH GOT"
4. After writing the required package data to the GOT, refer to the <How to check the versions in use> and check that the software has been updated to the fixed versions.

1 https://www.first.org/cvss/v3.1/specification-document
2 https://cwe.mitre.org/data/definitions/20.html

■Mitigations

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

・When Internet access is required, use a virtual private network (VPN) or other means to prevent unauthorized access.
・Use the products within a LAN and block access from untrusted networks and hosts.
・Install antivirus software on your computer with the products installed.
・Set strong passwords to prevent unauthorized login by malicious attackers.
・Use the IP filter function*1 to restrict the accessible IP addresses.
*1: GT Designer3 (GOT2000) Screen Design Manual (SH-081220ENG). “5.4.3 Setting the IP filter”

■Contact information

Please contact your local Mitsubishi Electric representative.

< Inquiries | MITSUBISHI ELECTRIC FA >
https://www.mitsubishielectric.com/fa/support/index.html