Denial-of-Service (DoS) and Spoofing Vulnerability in FTP Server Function on GOT2000 Series and GOT SIMPLE Series

Release date: August 3, 2023
Mitsubishi Electric Corporation

■Overview

Denial-of-Service (DoS) and spoofing (session hijacking of data connections) vulnerability caused by easily guessable port numbers of data connections exists in the FTP server function on GOT2000 Series and GOT SIMPLE Series. This vulnerability allows an attacker to hijack data connections (session hijacking) or prevent legitimate users from establishing data connections (to cause DoS condition) by guessing the listening port of the data connection on FTP server and connecting to it. (CVE-2023-3373)

■CVSS[1]

CVE-2023-3373 CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:L Base Score:5.9

■Affected products

Affected products and versions are listed below.

Affected when using the "FTP server" function

Series	Model	Affected Base System Application versions
GOT2000 Series	GT21 model	01.49.000 and prior
GOT SIMPLE	GS21 model	01.49.000 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) and spoofing (session hijacking of data connections) vulnerability (CVE-2023-3373) exists in the FTP server function on GOT2000 Series and GOT SIMPLE Series because the port number of a data connection can be easily guessed due to Predictable Exact Value from Previous Values (CWE-342)[2].

■Impact

The vulnerability allows an attacker to hijack data connections (session hijacking) or prevent legitimate users from establishing data connections (to cause DoS condition) by guessing the listening port of the data connection on FTP server and connecting to it.

■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.
(The fixed versions are shipped with GT Designer3 Version1(GOT2000) Ver. 1.300 N or later)

Series	Model	Affected Base System Application versions
GOT2000 Series	GT21 model	01.50.000 or later
GOT SIMPLE	GS21 model	01.50.000 or later

[1] https://www.first.org/cvss/v3.1/specification-document

[2] https://cwe.mitre.org/data/definitions/342.html

<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.

■Mitigations / Workarounds

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

[Mitigations]

・Restrict physical access to the product and the LAN to which it is connected.
・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 that can access the affected product.
・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"

[Workarounds]

・Review whether the FTP server function is required or not, and if not, disable the FTP server function.

■Contact information

Please contact your local Mitsubishi Electric representative.

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