Multiple vulnerabilities in TCP/IP Stack on GOT2000 Series

July 3rd, 2020
Mitsubishi Electric Corporation

■Overview

There are multiple vulnerabilities in TCP/IP stack of the firmware in GT27 model, GT25 model and GT23 model of GOT2000 series with CoreOS version ‘-Y’ and earlier. If these vulnerabilities are exploited by malicious attackers, the network functions of the products may enter a denial-of-service condition or malware may be executed.

■How to check affected products

Affected products are as follows

【Affected products and version】.

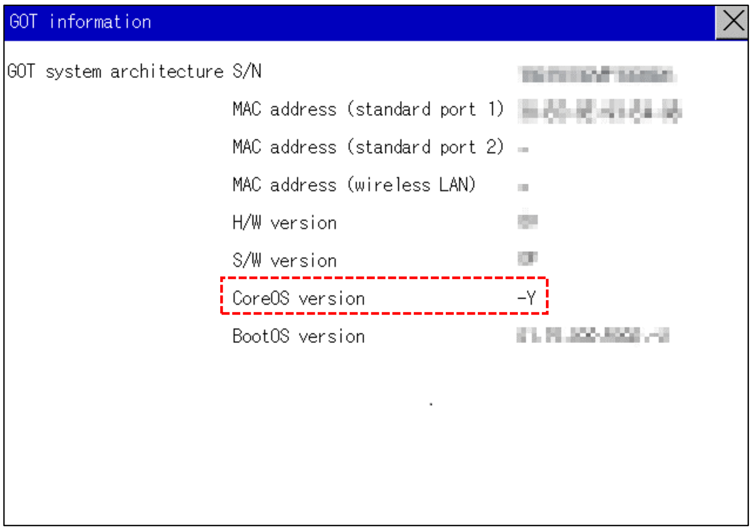
CoreOS version ‘-Y’ and earlier for the following models

GT27 Model
GT25 Model
GT23 Model

【How to check the used versions】

Procedure for confirming version information is as follows.

1) Start GOT
2) Select [Utility main menu] and [Maintenance].
3) Select [GOT information]
4) Check the [Core OS Version] in the GOT information Window. (Ref. Fig1)



GOT system architecture	S/N	[redacted]
	MAC address (standard port 1)	[redacted]
	MAC address (standard port 2)	[redacted]
	MAC address (wireless LAN)	[redacted]
	H/W version	[redacted]
	S/W version	[redacted]
	CoreOS version	-Y
	BootOS version	[redacted]

Fig1: GOT information Window

■Description

There are following multiple vulnerabilities in TCP/IP stack of the firmware in GT27 model, GT25 model and GT23 model of GOT2000 series. By receiving a malicious attack from remote attackers, the network functions of the products may enter a denial-of-service condition or malware may be executed.

·Improper Restriction of Operations within the Bounds of a Memory Buffer (CWE-119) CVE-2020-5595
·Session Fixation (CWE-384) CVE-2020-5596
·NULL Pointer Dereference (CWE-476) CVE-2020-5597
·Improper Access Control (CWE-284) CVE-2020-5598
·Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') (CWE-88) CVE-2020-5599
·Resource Management Errors (CWE-399)CVE-2020-5600

■Impact

By receiving specially crafted TCP/IP packets from attackers, the network functions of the products may enter a denial-of-service condition or malware may be executed.

■Countermeasures

In the case of using the affected products and versions, please update to the fixed versions by following the steps below.

【Fixed versions】

Core OS version -Z and later [MELSOFT GT Designer3(2000) version 1.240A and later]

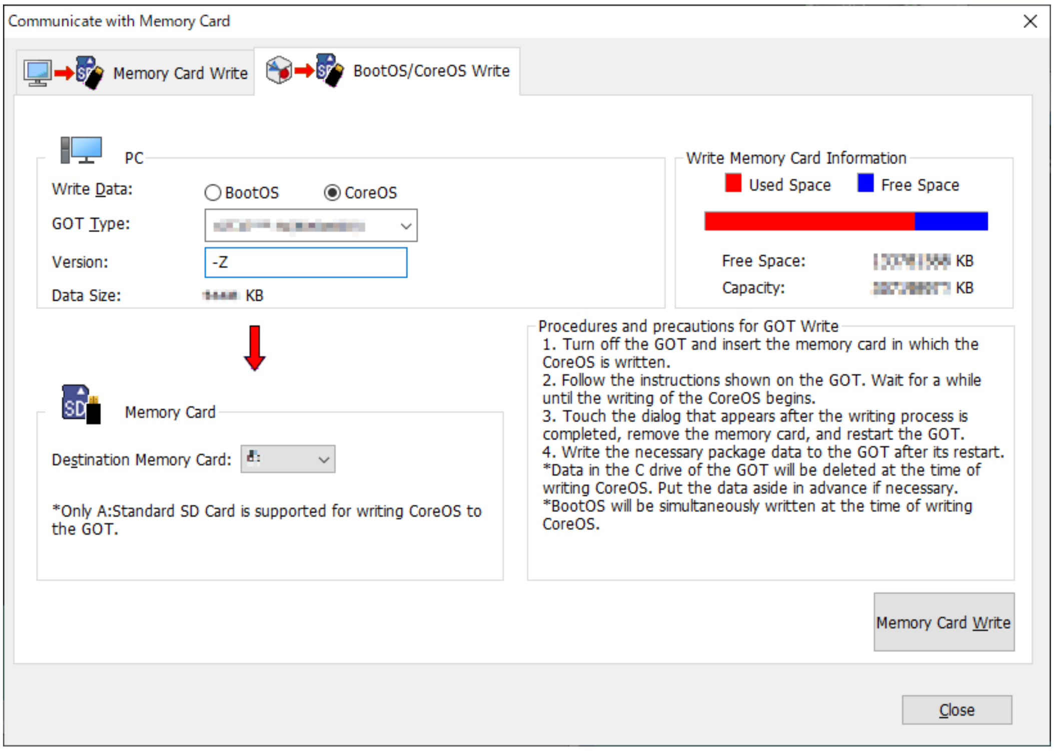
Note: When the CoreOS is installed, all the data in the GOT are deleted.
If the data in the GOT is required, backup the data in advance.

1) Download the fixed version of MELSOFT GT Designer3(2000) and install into the PC.
Please contact your local sales office about MELSOFT GT Designer3(2000).

2) Please insert the SD card into the computer, start the MELSOFT GT Designer3 and select [Transfer to memory card] from [Communication] menu.

3) After the [Communicate with Memory Card] window is displayed, please select the following contents. (Ref Fig2)

Write Type	:Select the [BootOS/CoreOS Write] tab
Write Data	:Select the [CoreOS]
GOT Type	:Select the type of the destination GOT for [GOT Type]
Destination Memory Card	:Set the drive letter of SD Card which is inserted in your PC.



Write Data: ○ BootOS ● CoreOS

GOT Type: [redacted]

Version: -Z

Data Size: [redacted] KB

Free Space: [redacted] KB

Capacity: [redacted] KB

Destination Memory Card: [redacted]

*Only A:Standard SD Card is supported for writing CoreOS to the GOT.

Procedures and precautions for GOT Write

1. Turn off the GOT and insert the memory card in which the CoreOS is written.
2. Follow the instructions shown on the GOT. Wait for a while until the writing of the CoreOS begins.
3. Touch the dialog that appears after the writing process is completed, remove the memory card, and restart the GOT.
4. Write the necessary package data to the GOT after its restart.
*Data in the C drive of the GOT will be deleted at the time of writing CoreOS. Put the data aside in advance if necessary.
*BootOS will be simultaneously written at the time of writing CoreOS.

Fig2: Communicate with Memory Card Window

4) Click the [Memory Card Write] button

5) After the writing to the SD Card is completed, remove the SD Card from your PC and insert it into the GOT.

6) Turn on the GOT.

7) The confirmation message for installing the CoreOS appears.
To install the CoreOS, touch the screen for two seconds or longer.
To abort the installation of the CoreOS, turn off the GOT.

8) When the installation of the CoreOS is completed, the completion message appears.
Touch the screen to restart the GOT.

9) Write the required package data to the restarted GOT.

After write the required package data to the GOT, refer to the【How to check the used versions】and check the fixed versions.

※Please refer to the GT Designer3 (GOT2000) Screen Design Manual.

■Mitigations

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

■Contact information

Please contact your local Mitsubishi Electric representative.