Multiple vulnerabilities in TCP/IP Stack on GT14 Model of GOT1000 Series

Release date: November 5, 2020
Mitsubishi Electric Corporation

■Overview

There are multiple vulnerabilities in TCP/IP stack of the firmware in GT14 model of GOT1000 series with CoreOS version '05.65.00.BD' 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.
（CVE-2020-5644、CVE-2020-5645、CVE-2020-5646、CVE-2020-5647、CVE-2020-5648、CVE-2020-5649）

■CVSS

CVE-2020-5644	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	Base Score:9.8
CVE-2020-5645	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	Base Score:7.5
CVE-2020-5646	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	Base Score:7.5
CVE-2020-5647	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	Base Score:9.8
CVE-2020-5648	CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H	Base Score:7.1
CVE-2020-5649	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	Base Score:5.3

■How to check affected products

Affected products are as follows

【Affected products and version】.

CoreOS version '05.65.00.BD' and earlier for the following models

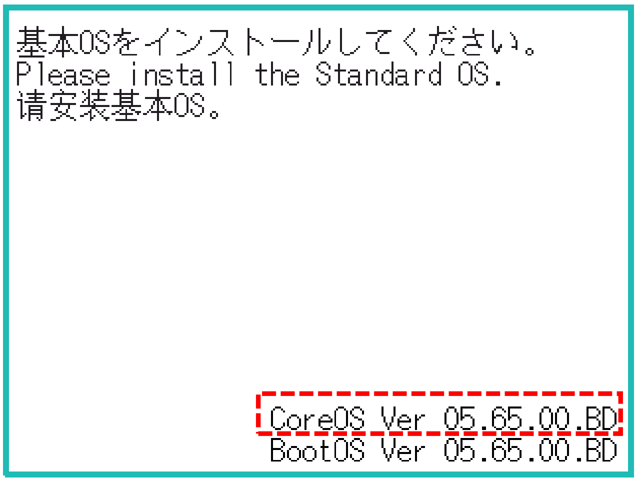
- ・GT1455-QTBDE
- ・GT1450-QMBDE
- ・GT1450-QLBDE
- ・GT1455HS-QTBDE
- ・GT1450HS-QMBDE

【How to check the used versions】

You can check which version you are using by the following way.

The screen shown in Fig 1 will be displayed in the following state.

- ・GOT in the same condition as it was shipped from the factory.
- ・GOT with BootOS only installed.
- ・With SD card and USB memory not inserted, power on the GOT while pressing upper left corner of the GOT screen.
  If the CoreOS version is not displayed, it is the affected version.



基本OSをインストールしてください。
Please install the Standard OS.
请安装基本OS。

CoreOS Ver 05.65.00.BD
BootOS Ver 05.65.00.BD

[Fig 1 Factory Shipment Display Screen]

■Description

There are following multiple vulnerabilities in TCP/IP stack of the firmware in GT14 model of GOT1000 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-2020-5644
- ･Session Fixation (CWE-384) CVE-2020-5645
- ･NULL Pointer Dereference (CWE-476) CVE-2020-5646
- ･Improper Access Control (CWE-284) CVE-2020-5647
- ･Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') (CWE-88) CVE-2020-5648
- ･Resource Management Errors (CWE-399) CVE-2020-5649

■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 “05.76.00.BG” and later [MELSOFT GT Designer3 Version1(GOT1000) version 1.245F and later]

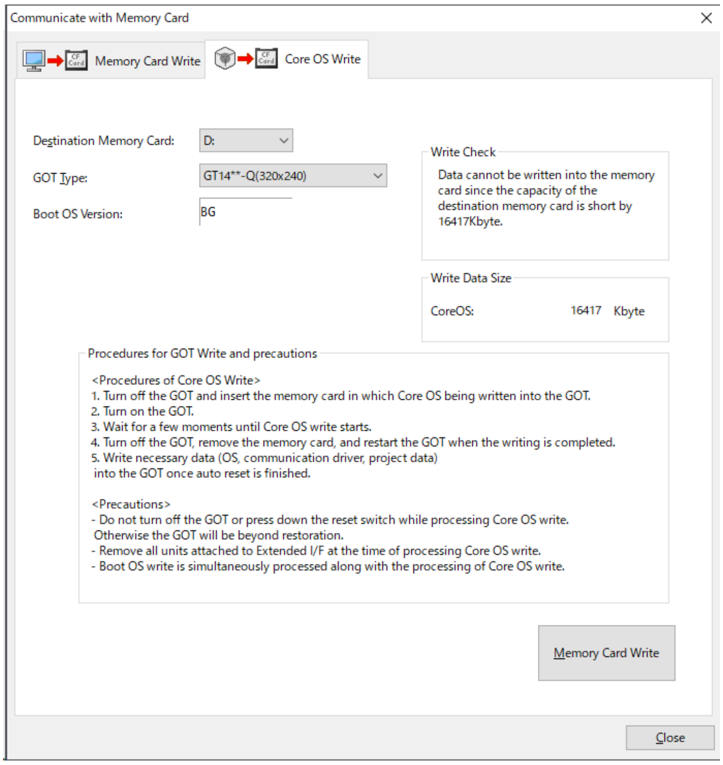
Note : When the CoreOS is installed, all the data in the GOT are deleted.
If the data in the GOT is required, backup the data in advance.

① Download the fixed version of MELSOFT GT Designer3 Version1(GOT1000) and install into the PC.
Please contact your local sales office about MELSOFT GT Designer3 Version1(GOT1000).

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. (Fig 2)

･Write Type	:Select the [CoreOS Write] tab
･Destination Memory Card	:Set the drive letter of SD Card which is inserted in your PC.
･GOT Type	:GT14**-Q(320×240)



Destination Memory Card: D:

GOT Type: GT14**-Q(320x240)

Boot OS Version: BG

Write Check

Data cannot be written into the memory card since the capacity of the destination memory card is short by 16417Kbyte.

Write Data Size

CoreOS: 16417 Kbyte

Procedures for GOT Write and precautions

<Procedures of Core OS Write>
1. Turn off the GOT and insert the memory card in which Core OS being written into the GOT.
2. Turn on the GOT.
3. Wait for a few moments until Core OS write starts.
4. Turn off the GOT, remove the memory card, and restart the GOT when the writing is completed.
5. Write necessary data (OS, communication driver, project data)
into the GOT once auto reset is finished.

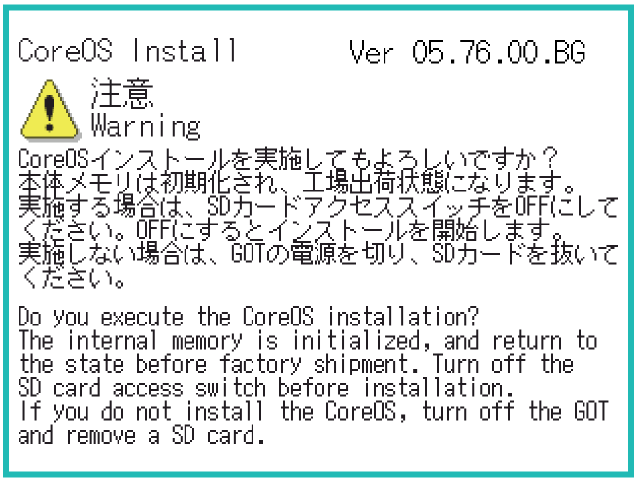
<Precautions>
- Do not turn off the GOT or press down the reset switch while processing Core OS write.
Otherwise the GOT will be beyond restoration.
- Remove all units attached to Extended I/F at the time of processing Core OS write.
- Boot OS write is simultaneously processed along with the processing of Core OS write.

[Fig 2 CoreOS Write Window]

④ Click the [Memory Card Write] button.

⑤ After confirming that the GOT is powered off, insert the SD card to the GOT.
After inserting, turn on the SD card access switch.

⑥ Powering on the GOT to display the installation screen. (Fig 3)
To cancel the installation, power off the GOT and remove the SD card.



CoreOS Install Ver 05.76.00.BG

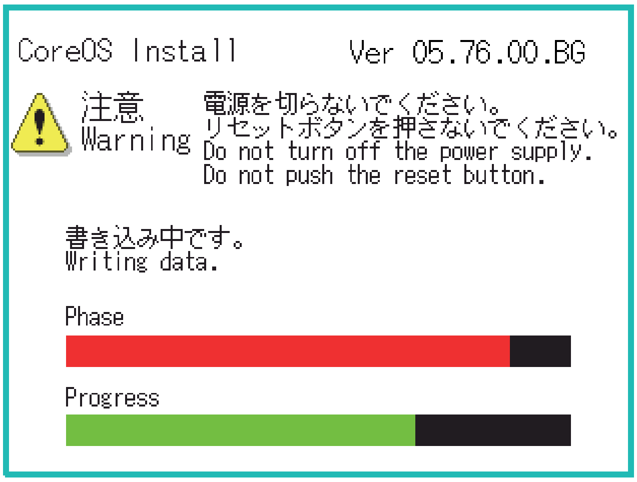
注意
Warning

CoreOSインストールを実施してもよろしいですか？
本体メモリは初期化され、工場出荷状態になります。
実施する場合は、SDカードアクセススイッチをOFFにして
ください。OFFにするとインストールを開始します。
実施しない場合は、GOTの電源を切り、SDカードを抜いて
ください。

Do you execute the CoreOS installation?
The internal memory is initialized, and return to
the state before factory shipment. Turn off the
SD card access switch before installation.
If you do not install the CoreOS, turn off the GOT
and remove a SD card.

[Fig 3 CoreOS Write Start Display Screen]

⑦ Turning off the SD card access switch to start the CoreOS installation. (Fig 4)
Note : During installation, do not power off the GOT.



CoreOS Install Ver 05.76.00.BG

注意
Warning

電源を切らないでください。
リセットボタンを押さないでください。
Do not turn off the power supply.
Do not push the reset button.

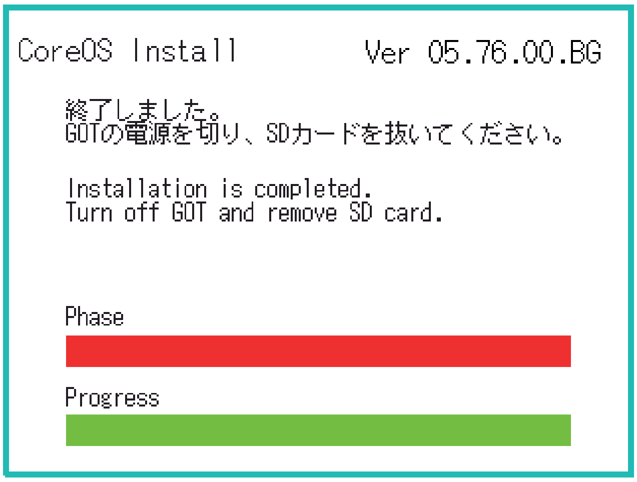
書き込み中です。
Writing data.

Phase

Progress

[Fig 4 CoreOS Write Execution Display Screen]

⑧ When the installation of the CoreOS is completed, the completion message appears. (Fig 5)
The POWER LED of the GOT blinks (green/orange) at the installation completion.
Confirm that the message is displayed and power off the GOT.

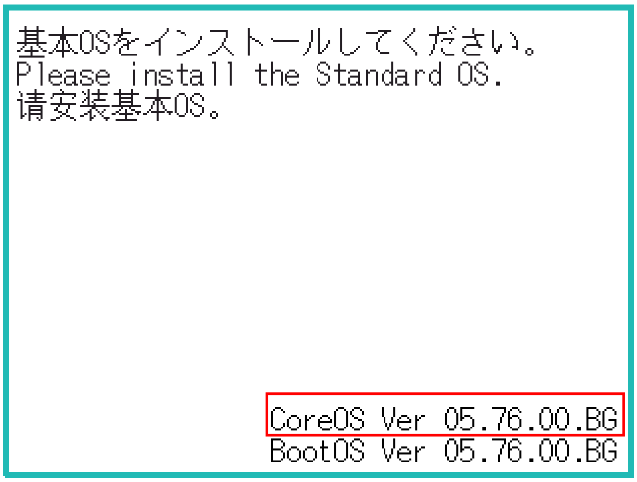


```
CoreOS Install          Ver 05.76.00.BG

   終了しました。
   GOTの電源を切り、SDカードを抜いてください。

   Installation is completed.
   Turn off GOT and remove SD card.


   Phase

   Progress
```

[Fig 5 CoreOS Write Completion Display Screen]

⑨ Remove the SD card after powering the GOT off.

⑩ Powering on the GOT again displays the screen. (Fig 6)
Please confirm whether the version of CoreOS is “05.76.00.BG” or later.



```
基本OSをインストールしてください。
Please install the Standard OS.
请安装基本OS。



                CoreOS Ver 05.76.00.BG
                BootOS Ver 05.76.00.BG
```

[Fig 6 Factory Shipment Display Screen]

⑪ Install OS (Standard monitor OS, communication driver, etc.) and install project data as required.
Please refer to the GT14 User’s Manual or the GT14 Handy GOT User’s Manual.

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

■Contact information
Please contact your local Mitsubishi Electric representative.