Multiple vulnerabilities in TCP/IP function on MELSEC C Controller Module and MELIPC Series MI5000

February 14th, 2020
Mitsubishi Electric Corporation

■Overview

Multiple vulnerabilities were found in TCP/IP function (IPnet) of VxWorks version 6.5 and later, a real-time OS distributed by Wind River. Services of the affected product may stop or a malicious program may be executed if it receives a TCP packet crafted by a remote attacker when it is connected to a network.
The versions of MELSEC C Controller Module and MELIPC Series MI5000 that are affected by the vulnerability are listed as follows. In the case of using the affected products, take defensive measures described in the Countermeasures or Mitigations to minimize the risk of exploitation of the vulnerability.

■Affected products

Affected products and Ethernet ports are as follows.

[MELSEC-Q Series C Controller Module]
-Q24DHCCPU-V, Q24DHCCPU-VG User Ethernet port (CH1, CH2): First 5 digits of serial number are 21121 or before.

The serial number of CPU module can be checked on a rating plate on the side of the module or serial number display on the front of the module, or checked in "System monitor" of Setting/monitoring tools for the MELSEC C Controller Module.

[MELSEC iQ-R Series C Controller Module / C Intelligent Function Module]
-R12CCPU-V Ethernet port (CH1, CH2): First 2 digits of serial number are 11 or before.

The serial number of CPU module can be checked on a rating plate on the side of the module or serial number display on the front of the module, or checked in "System monitor" of CW Configurator.

-RD55UP06-V Ethernet port: First 2 digits of serial number are 08 or before.

The serial number of CPU module can be checked on a rating plate on the side of the module or serial number display on the front of the module, or checked in "System monitor" of GX Works3.

[MELIPC Series MI5000]
-MI5122-VW Ethernet port (CH1): First 2 digits of serial number are 03 or before.

The serial number of CPU module can be checked on a rating plate on the side of the module or serial number display on the front of the module, and the firmware version can be checked in "MELIPC Diagnosis" of MI Configurator.

■Description

MELSEC C controller Module and MELIPC Series MI5000 have the following multiple vulnerabilities due to the TCP/IP function (IPnet) of VxWorks, a real-time OS distributed by Wind River.:

-Q24DHCCPU-V, Q24DHCCPU-VG
  CVE-2019-12255/12257/12258/12259/12261/12262/12263/12264/12265
-R12CCPU-V, RD55UP06-V
  CVE-2019-12256/12258/12259/12261/12262/12263/12264/12265
-MI5122-VW
  CVE-2019-12256/12258/12259/12260/12261/12262/12263/12264/12265

■Impact

Receiving a TCP packet crafted by a remote attacker may cause service of the product to stop or a malicious program to execute.

■Countermeasures

We have fixed the vulnerabilities due to the TCP/IP function (IPnet) at the following versions to improve security of the products.

[MELSEC-Q Series C Controller Module]
- Q24DHCCPU-V, Q24DHCCPU-VG: First 5 digits of serial number are “21122” or later.

[MELSEC iQ-R Series C Controller Module / C Intelligent Function Module]
- R12CCPU-V: First 2 digits of serial number are “12” or later.
- RD55UP06-V: First 2 digits of serial number are “09” or later.

[MELIPC Series MI5000]
- MI5122-VW: First 2 digits of serial number are “04” or later, or the firmware version is “04” or later.

■Mitigations

Please restrict access to the product only from trusted networks.

■Contact information

Please contact your local Mitsubishi Electric representative.