TECHNICAL BULLETIN

FA-A-0297-A

Vulnerabilities in TCP/IP Function on MELSEC C Controller Modules and MELIPC MI5000

■Date of Issue

March 2020

■Relevant Models

R12CCPU-V, RD55UP06-V

Q24DHCCPU-V, Q24DHCCPU-VG

MI5122-VW

Thank you for your continued support of MELSEC and MELIPC series.
We will inform you that multiple vulnerabilities resulting from the TCP/IP function (IPnet) of VxWorks® version 6.5 and later, which is a real-time operation system manufactured by Wind River®, were found in MELSEC C Controller modules, C intelligent function modules, and MELIPC MI5000.
Please take measures against the vulnerabilities as described below.
The product used within trusted networks is not affected by the vulnerabilities.

1 RELEVANT MODELS

The following shows products and Ethernet ports that are affected by the vulnerabilities.

Product name		Model	Version information		Ethernet port
MELSEC iQ-R	C Controller module	R12CCPU-V	• First two digits of the product information (16 digits)[*1] • Firmware version	'11' or earlier	Ethernet port (CH1 and CH2)
	C intelligent function module	RD55UP06-V	• First two digits of the product information (16 digits)[*1] • Firmware version	'08' or earlier	Ethernet port
MELSEC-Q	C Controller module	Q24DHCCPU-V	First five digits of the serial number	'21121' or earlier	User Ethernet port (CH1 and CH2)
		Q24DHCCPU-VG			
MELIPC	MI5000	MI5122-VW	• First two digits of the product information (16 digits) • Firmware version	'03' or earlier	Ethernet port (CH1)

[*1] After updating the firmware, check the firmware version.

Point

Product information, firmware versions, or serial numbers can be checked with the followings:

- Rating plate
- Production information marking or serial number display
- System monitor of a software package for each product

For details on the checking methods, refer to the user's manual of the product being used or MELSEC iQ-R Module Configuration Manual.

2 IMPACT

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

For details, refer to the following:

Website	URL
ICS-CERT (Industrial Control Systems Cyber Emergency Response Team)	www.us-cert.gov/ics/advisories/icsa-19-274-01
JVN (Japan Vulnerability Notes)	jvn.jp/en/vu/JVNVU95424547

3 CORRECTIVE ACTION

3.1 Measures for Products

To enhance security, countermeasures for TCP/IP function vulnerabilities are implemented in the products with the following versions:

Product name		Model	Version information	
MELSEC iQ-R	C Controller module	R12CCPU-V	• First two digits of the product information (16 digits) • Firmware version	'12' or later
	C intelligent function module	RD55UP06-V	• First two digits of the product information (16 digits) • Firmware version	'09' or later
MELSEC-Q	C Controller module	Q24DHCCPU-V	First five digits of the serial number	'21122' or later
		Q24DHCCPU-VG		
MELIPC	MI5000	MI5122-VW	• First two digits of the product information (16 digits) • Firmware version	'04' or later

3.2 Mitigation Measures Taken by Users

Please restrict access to the product only from trusted networks.

REVISIONS

Version	Date of Issue	Revision
A	March 2020	First edition

TRADEMARK

VxWorks and Wind River are either registered trademarks or trademarks of Wind River Systems, Inc.

The company names, system names and product names mentioned in this bulletin are either registered trademarks or trademarks of their respective companies.

In some cases, trademark symbols such as '™' or '®' are not specified in this bulletin.