MITSUBISHI ELECTRIC

技术简讯

FA-CN-0297-A

关于MELSEC C语言控制器模块与MELIPC MI5000中的TCP/IP功能的脆弱性

■出版年月

2020年3月

■相关机型

R12CCPU-V、RD55UP06-V

Q24DHCCPU-V、Q24DHCCPU-VG

MI5122-VW

感谢您继续支持MELSEC与MELIPC系列的产品。

此次，判明了MELSEC C语言控制器模块、C语言智能功能模块，以及MELIPC MI5000中存在多个由Wind River®生产的6.5及之后版本的实时操作系统VxWorks®的TCP/IP功能 （IPnet）引起的脆弱性。

本技术简讯中，对于脆弱性的概要及客户方面的应对方法进行了如下所示的介绍，敬请关注。

若仅通过可信任的网络进行访问，则不会发生本次介绍的脆弱性。

1 对象产品

受脆弱性影响的产品及其对应的以太网端口如下所示。

产品名		型号	版本信息		以太网端口
MELSEC iQ-R	C语言控制器模块	R12CCPU-V	• 生产信息 （16位）的前两位*1 • 固件版本	11及之前	以太网端口 （CH1、CH2）
	C语言智能功能模块	RD55UP06-V	• 生产信息 （16位）的前两位*1 • 固件版本	08及之前	以太网端口
MELSEC-Q	C语言控制器模块	Q24DHCCPU-V	序列号的前5位	21121及之前	用户以太网端口 （CH1、CH2）
		Q24DHCCPU-VG			
MELIPC	MI5000	MI5122-VW	• 生产信息 （16位）的前两位 • 固件版本	03及之前	以太网端口 （CH1）

*1 执行固件更新时应确认固件版本。

要点

可通过以下内容确认生产信息、固件版本或序列号。

- 额定显示部/额定铭牌
- 生产信息显示部/序列号显示部
- 所支持的软件包的系统监视

关于确认方法的详细说明，请参阅所使用产品的用户手册或MELSEC iQ-R 模块配置手册。

2 脆弱性的内容

若接收了由攻击者制作的TCP数据包，则可能导致产品服务停止，或恶意程序被执行。
关于详细说明，请参阅以下内容。

网站	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 处理方法

3.1 产品方面的处理

为了增强安全性，已在以下版本的产品中执行了TCP/IP功能的脆弱性对策。

产品名		型号	版本信息	
MELSEC iQ-R	C语言控制器模块	R12CCPU-V	• 生产信息（16位）的前两位 • 固件版本	12及之后
	C语言智能功能模块	RD55UP06-V	• 生产信息（16位）的前两位 • 固件版本	09及之后
MELSEC-Q	C语言控制器模块	Q24DHCCPU-V	序列号的前5位	21122及之后
		Q24DHCCPU-VG		
MELIPC	MI5000	MI5122-VW	• 生产信息（16位）的前两位 • 固件版本	04及之后

3.2 客户方面的应对措施

应仅通过可信任的网络访问产品。

修订记录

副编号	修订年月	修订内容
A	2020年3月	第一版

商标