MITSUBISHI ELECTRIC

技术简讯

FA-CN-0313-A

关于MELSEC iQ-R系列以太网端口搭载模块的以太网通信停止的脆弱性

■出版年月

2020年8月

■相关机型

Rn(EN)CPU、RnSFCPU、RnP(SF)CPU、RJ71EN71

感谢您继续支持三菱电机MELSEC iQ-R系列可编程控制器。

判明了在MELSEC iQ-R系列以太网端口搭载模块*1中存在以太网通信停止的脆弱性。本技术简讯中，对于脆弱性的概要及客户的对应方法进行了如下所示的介绍，敬请关注。

*1 表示搭载了以太网连接器的模块。

1 对象产品

受脆弱性影响的产品如下所示。

产品名称	型号	固件版本*1
可编程控制器CPU	R00CPU、R01CPU、R02CPU	07及以前
	R04CPU、R08CPU、R16CPU、R32CPU、R120CPU、R04ENCPU、R08ENCPU、R16ENCPU、R32ENCPU、R120ENCPU	39及以前
安全CPU	R08SFCPU、R16SFCPU、R32SFCPU、R120SFCPU	20及以前
过程CPU	R08PCPU、R16PCPU、R32PCPU、R120PCPU	所有版本
SIL2过程CPU	R08PSFCPU、R16PSFCPU、R32PSFCPU、R120PSFCPU	所有版本
以太网模块	RJ71EN71	所有版本

*1 实施了固件更新时，应确认固件版本。

要点

关于固件版本，可通过工程工具的系统监视进行确认。
确认方法的详细内容，请参照MELSEC iQ-R 模块配置手册。

2 脆弱性的内容

在MELSEC iQ-R系列以太网端口搭载模块中，如果在短时间内大量接收攻击者加工的数据包，则以太网通信有可能停止。
详细内容请参照下述网站。

网站	URL
ICS-CERT(Industrial Control Systems Cyber Emergency Response Team)	us-cert.cisa.gov/ics/advisories/icsa-20-161-02
JPCERT(Japan Computer Emergency Response Team)	jvn.jp/vu/JVNVU97662844/

3 处理方法

3.1 模块上的处理

为了强化模块的安全，在下述版本的产品中对应了以太网通信继续运行。

产品名称	型号	固件版本
可编程控制器CPU	R00CPU、R01CPU、R02CPU	08及以后
	R04CPU、R08CPU、R16CPU、R32CPU、R120CPU、R04ENCPU、R08ENCPU、R16ENCPU、R32ENCPU、R120ENCPU	40及以后
安全CPU	R08SFCPU、R16SFCPU、R32SFCPU、R120SFCPU	21及以后

关于上述以外的模块，预计近期进行对应。应实施“☞ 3页 客户的对策”。

3.2 客户的对策

对于来自经由网络的外部设备的非法访问，应采取防火墙等的防范措施。

对于客户所使用的装置有无连接网络及有无防火墙等的防范措施，应向IT管理部门或装置交付对象等进行确认。

项目	内容
有无连接网络的确认	应确认所使用的装置中安装的模块有无连接网络。
防火墙防范措施等的确认	有经由无法信任的网络及主机的通信的情况下，应通过防火墙对来自无法信任的网络及主机的访问进行拦截。

修订记录

副编号	修订年月	修订内容
A	2020年8月	第一版

商标