MITSUBISHI ELECTRIC

技术简讯 [1 / 3]

FA-CN-0290-A

关于MELSEC-Q系列CPU模块及MELSEC-L系列CPU模块的FTP服务器功能的脆弱性

■出版年月

2019年12月

■相关机型

以太网端口内置QCPU、以太网端口内置LCPU

感谢您继续支持三菱电机MELSEC-Q系列及MELSEC-L系列可编程控制器。

此次，判明了MELSEC-Q系列CPU模块及MELSEC-L系列CPU模块中存在FTP服务器功能的脆弱性。本技术简讯中，对于脆弱性的概要及客户方面的对应方法进行了如下所示的介绍，敬请关注。

1 脆弱性的概要

对象产品

机型名称	型号	序列号的前5位
以太网端口内置QCPU	• Q03UDVCPU • Q03UDECPU • Q04UD(P)VCPU • Q04UDEHCPU • Q06UD(P)VCPU • Q06UDEHCPU • Q10UDEHCPU • Q13UD(P)VCPU • Q13UDEHCPU • Q20UDEHCPU • Q26UD(P)VCPU • Q26UDEHCPU • Q50UDEHCPU • Q100UDEHCPU	“21081”及之前
以太网端口内置LCPU	• L02CPU(-P) • L06CPU(-P) • L26CPU(-P) • L26CPU-(P)BT	“21101”及之前

脆弱性的内容

MELSEC-Q系列CPU模块及MELSEC-L系列CPU模块中存在FTP服务器的资源枯竭 （CWE-400）的脆弱性。根据攻击者连接到相应产品的FTP服务器的时机，可能使FTP服务陷入DoS状态*1，并导致正常的FTP客户端无法连接到FTP服务器。但是，本脆弱性不会对FTP服务器以外的功能产生影响。

*1 DoS （Denial of Service）状态是指，由于攻击者导致该服务的运行受到阻碍的状态。

（参考）外部机关发布URL

外部机关	URL
ICS-CERT （Industrial Control Systems Cyber Emergency Response Team）	ics-cert.us-cert.gov/advisories/ICSA-19-311-01
JPCERT/CC （Japan Computer Emergency Response Team Coordination Center）	jvn.jp/vu/JVNVU97094124/

2 恢复方法

由于本脆弱性导致无法连接到FTP服务器的情况下，可通过以下任意一种方法进行恢复。

• 通过GX Works2的“以太网诊断”画面的“各连接状态”标签强制禁用FTP服务器后再解除禁用。

[诊断]⇨[以太网诊断]

• 从CPU模块拔出以太网电缆，1分钟之后再连接。

3 客户方面的对策

对于来自经由互联网的外部设备的非法访问，如三菱电机手册*1*2的[设计注意事项]中的“警告”所介绍，需要采取防火墙等防范措施。对于客户所使用的装置有无连接互联网及有无防火墙等防范措施，应向IT管理部门或装置交货对象等进行确认。

项目	内容
有无连接互联网	应确认所使用的装置中安装的CPU模块有无连接互联网。
防火墙防范措施等	连接了互联网的情况下，应确认是否采取了防火墙等防范措施。

*1 QnUCPU用户手册 （内置以太网端口通信篇）

*2 MELSEC-L CPU模块用户手册 （内置以太网功能篇）

4 CPU模块中的处理

为了强化CPU模块的安全，采取了一定时间没有来自FTP客户端的操作时自动切断连接的措施。

• 对应机型

机型名称	序列号的前5位
MELSEC-Q系列 CPU模块	“21082”及之后
MELSEC-L系列 CPU模块	“21102”及之后

修订记录

副编号	修订年月	修订内容
A	2019年12月	第一版