可编程控制器 CS/CJ 系列中

文件系统缺乏验证的漏洞

发布日期 2023 年 04 月 17 日

欧姆龙株式会社

■概要

欧姆龙一直致力于在工业自动化领域为客户提供安全、可靠、高质量的产品与解决方案，这是我们立足行业，持续助推客户业务增长，为客户创造价值的根基。

近期，我们发现在可编程控制器 CS/CJ 系列中，存在“关键功能缺乏验证（CWE-306)”的漏洞。攻击者可能会利用该漏洞，无需认证即可访问 CPU 单元提供的文件系统（存储卡或 EM 文件存储器)，窃取机密信息。

为了使您的安全得到有效保护，我们第一时间采取行动，排查受该漏洞影响的产品和版本，并推出相应对策、以及减轻措施/解决方法。您可以通过下述推荐的减轻措施/解决方法，实现将该漏洞的恶意利用风险降至最低。

■对象产品

受本漏洞影响的产品型号及版本如下：

系列	型号	适用版本
可编程控制器 SYSMAC CJ 系列	CJ2H-CPU6□-EIP CJ2H-CPU6□	所有版本
	CJ2M-CPU□□	所有版本

	CJ1G-CPU□□P	所有版本
SYSMAC CS 系列	CS1H-CPU□□H CS1G-CPU□□H	所有版本
	CS1D-CPU□□HA CS1D-CPU□□H	所有版本
	CS1D-CPU□□SA CS1D-CPU□□S	所有版本
	CS1D-CPU□□P	所有版本

■漏洞内容

在可编程控制器 CS/CJ 系列中，存在“关键功能缺乏验证（CWE-306)”的漏洞。

■漏洞可能造成的威胁

攻击者可能会利用该漏洞,无需认证即可访问 CPU 单元提供的文件系统(存储卡或 EM 文件存储器),窃取机密信息。

■CVSS 评分

关键功能缺乏验证（CWE-306）

CVE-2022-45794

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N 基础评分 7.5

■减轻措施/解决方法

为将该漏洞的恶意利用风险降至最低，建议采取以下减轻措施。

1.防止未经授权的访问

・最大限度地减少控制系统或设备的网络连接，禁止不受信任的设备访问。

・通过部署防火墙来隔离 IT 网络 (断开未使用的通信端口、限制通信主机、限制对 FINS 端口(9600)的访问)。

・需要远程访问控制系统或设备时，使用虚拟专用网络（VPN)。

・使用高强度密码并定期修改。

・引入物理控制，确保仅授权人员可访问控制系统和设备。

・在控制系统或设备中使用 USB 存储器等外部存储设备时，事先进行病毒扫描。

・在远程访问控制系统或设备时进行多重要素验证。

此外，使用如下所示的产品及版本时，也可通过启用 FINS 写保护功能，对写入采取措施。

系列	型号	对象版本	手册
可编程控制器 SYSMAC CJ 系列	CJ2H-CPU6□-EIP CJ2H-CPU6□	所有版本	参见 CJ 系列 CJ2 CPU Unit Software User's Manual (Cat. No. W473) 9-3-8 FINS Protection
	CJ2M-CPU□□	所有版本	
	CJ1G-CPU□□P	单元版本 2.0 以上	参见 CJ 系列 Programmable Controllers Operation Manual (Cat. No. W393). 1-7-3 Write Protection from FINS Commands Sent to CPU Units via Networks

SYSMAC CS 系列	CS1H-CPU□□H CS1G-CPU□□H	单元版本 2.0 以 上	参见 CS 系列 Programmable Controllers Operation Manual （Cat. No. W339） 1-7-3 Write Protection from FINS Commands Sent to CPU Units via Networks
	CS1D-CPU□□SA CS1D-CPU□□S	所有版本	参见 CS 系列 CS1D Duplex System Operation Manual （Cat. No. W405） 6-2-9 FINS Protection Tab Page (Single CPU Systems Only)

2.防病毒保护

在连接控制系统的电脑上安装最新版本的企业级杀毒软件，并定期维护。

3.数据输入/输出保护

确认备份和范围检查等设置的合理性，以防对控制系统和设备的输入/输出数据的意外修改。

4.恢复丢失的数据

定期对设置数据进行备份和维护，以防数据丢失。

■咨询方式

如您在采取减轻措施/解决方法时遇到问题，可以通过下列方式向我们的事务所或经销商咨询：

https://www.fa.omron.com.cn/contactus

■更新记录

2023/04/17 创建