

可编程控制器 CS/CJ/CP 系列 FINS 协议

存在交互频率控制不当漏洞

发布日期：2023 年 9 月 19 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，我们发现可编程控制器 CS/CJ/CP 系列 FINS 协议存在交互频率控制不当（CWE-799）漏洞。攻击者可利用本漏洞解除受密码保护的内存区域的保护，进而未经授权获取相应控制器产品中的信息。

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。

此外，为了确保您安心使用本产品，我们还为受该漏洞影响的产品准备了安全增强的对策版本。您可在下文“对策方法”处查找对应的对策版本。

■对象产品

受本漏洞影响的产品型号及版本如下所示。

| 产品名称 | 型号 | 适用版本 |
|--------------|------------------|------------|
| 可编程控制器 CJ 系列 | CJ2H-CPU□□(-EIP) | Ver.1.4 以下 |
| | CJ2M-CPU□□ | Ver.2.0 以下 |
| | CJ1G-CPU□□P | Ver.4.0 以下 |
| 可编程控制器 CS 系列 | CS1H-CPU□□H | Ver.4.0 以下 |
| | CS1G-CPU□□H | |
| | CS1D-CPU□□H | Ver.1.3 以下 |
| | CS1D-CPU□□P | |
| CS1D-CPU□□S | Ver2.0 以下 | |
| 可编程控制器 CP 系列 | CP1E-E | Ver.1.2 以下 |
| | CP1E-N | |

确认对象产品版本的方法请参见以下手册。

- CJ 系列 CJ2 CPU Unit User's Manual (Hardware) (W472)
- CJ 系列 Programable Controllers Operation Manual (W393)
- CS 系列 Programable Controllers Operation Manual (W339)
- CS 系列 CS1D Duplex system Operation Manual (W405)
- CP 系列 CP1E CPU Unit User's Manual (Hardware) (W479)

请参见以上手册中的“Checking Versions”部分。

■漏洞内容

可编程控制器 CS/CJ/CP 系列 FINS 协议存在交互频率控制不当（CWE-799）漏洞。攻击者可利用本漏洞非法访问该产品并进行操作。

■漏洞可能造成的威胁

攻击者可通过 FINS 协议连续快速的多次调出“解除内存区域保护”，以解除受密码保护的内存区域的保护，进而未经授权获取相应控制器产品中的信息。

■CVSS 评分

交互频率控制不当（CWE-799）

CVE-2022-45790

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

为了实现将这些漏洞的恶意利用风险降至最低，我们十分建议您采取以下减轻措施。

1. 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。

2. 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
- 通过部署防火墙隔离 IT 网络（断开未使用的通信端口、限制通信主机）
- 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

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

■对策方法

可将各产品更新至对策版本以应对漏洞。

各产品的对策版本与发布日期见下表。

| 产品名称 | 型号 | 对策版本 | 发布日期 | |
|--------------|------------------|------------|-------------|--|
| 可编程控制器 CJ 系列 | CJ2H-CPU□□(-EIP) | Ver.1.5 以上 | 已于 2016 年提供 | |
| | CJ2M-CPU□□ | Ver.2.1 以上 | | |
| | CJ1G-CPU□□P | Ver.4.1 以上 | | |
| 可编程控制器 CS 系列 | CS1H-CPU□□H | Ver.4.1 以上 | | |
| | CS1G-CPU□□H | | | |
| | CS1D-CPU□□H | Ver.1.4 以上 | | |
| | CS1D-CPU□□P | | | |
| | CS1D-CPU□□S | Ver2.1 以上 | | |
| 可编程控制器 CP 系列 | CP1E-E | Ver.1.3 以上 | | |
| | CP1E-N | | | |

上述对策版本的获取途径及更新方法，请通过下述咨询方式咨询本公司。

■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>

■谢辞

Dragos 公司的 Reid Wightman 先生通过 CISA 报告了本漏洞。

我们在此感谢发现并报告了漏洞的 Reid Wightman 先生。

■更新记录

2023 年 9 月 19 日创建