可编程控制器 CS/CJ/CP 系列的
通信功能和身份验证绕过漏洞

发布日期：2022 年 12 月 21 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/CP 系列中，存在“敏感信息的明文传输（CWE-319)”、及“对数据真实性的验证不充分（CWE-345)”的漏洞。攻击者可能会利用该漏洞非法访问该控制器产品。

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	对象版本
可编程控制器 SYSMAC CS 系列	CS1G/H-CPU□□H	单元版本 4.0 及以下
	CS1D-CPU□□S	单元版本 2.0 及以下
	CS1D-CPU□□H	单元版本 1.3 及以下
SYSMAC CJ 系列	CJ2H-CPU6□-EIP CJ2H-CPU6□	单元版本 1.4 及以下
	CJ2M-CPU□□	单元版本 2.0 及以下
SYSMAC CP 系列	CP1H-X40D□-□ CP1H-XA40D□-□ CP1H-Y20DT-D	单元版本 1.2 及以下
	CP1L-EL20D□-□ CP1L-EM□□D□-□ CP1L-L□□D□-□ CP1L-M□□D□-□	单元版本 1.0
	CP1E-E□□SD□-□ CP1E-N□□S□D□-□	单元版本 1.2 及以下

系列	型号	对象版本
	CP1E-E□□D□-□ CP1E-N□□D□-□ CP1E-NA□□D□-□	
FA 统合工具包 CX-One	CX-Programmer	版本 9.5 及以下

对象产品版本的确认方法请参阅以下手册

・CX-Programmer Ver.9.[] Operation Manual（W446-E1）

Refer to Unit Versions of CS/CJ/CP-series CPU Units

■漏洞内容

在可编程控制器 CS/CJ/CP 系列中，由于“敏感信息的明文传输（CWE-319)”及“对数据真实性的验证不充分（CWE-345)”的漏洞，存在可以非法访问该产品的漏洞。

■漏洞可能造成的威胁

攻击者可能会利用该漏洞，非法窃取密码，从而导致 PLC 的设置变更或信息泄露。

攻击者可能会利用该漏洞，通过绕过身份验证非法执行任意对象代码。

■CVSS 评分

（1）“敏感信息的明文传输（CWE-319)”引起的漏洞

CVE-2022-31204

CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N　基本评分：6.5

（2）“对数据真实性的验证不充分（CWE-345)”引起的漏洞

CVE-2022-31207

CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:H/A:H　基本评分：5.9

■减轻措施/解决方法

为了实现将该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.防止非法访问

· CVE-2022-31204 的减轻措施：使用以下产品和版本时，您可以设置扩展密码保护，从而降低密码被窃取的风险。

系列	型号	对象版本
可编程控制器 SYSMAC CS 系列	CS1G/H-CPU□□H	单元版本 4.1 及以上
	CS1D-CPU□□S	单元版本 2.1 及以上
	CS1D-CPU□□H	单元版本 1.4 及以上
SYSMAC CJ 系列	CJ2H-CPU6□-EIP CJ2H-CPU6□	单元版本 1.5 及以上
	CJ2M-CPU□□	单元版本 2.1 及以上
SYSMAC CP 系列	CP1H-X40D□-□ CP1H-XA40D□-□ CP1H-Y20DT-D	单元版本 1.3 及以上
	CP1L-EL20D□-□ CP1L-EM□□D□-□ CP1L-L□□D□-□ CP1L-M□□D□-□	单元版本 1.1 及以上
	CP1E-E□□SD□-□ CP1E-N□□S□D□-□ CP1E-E□□D□-□ CP1E-N□□D□-□ CP1E-NA□□D□-□	单元版本 1.3 及以上
FA 统合工具包 CX-One	CX-Programmer	版本 9.6 及以上

相关设置可参阅 CX-Programmer Ver.9.□Operation Manual（W446-E1）

Extended Protection Passwords (Option).

· CVE-2022-31207 的减轻措施：使用以下产品和版本时，您可以通过采取（1）和（2）措施，降低攻击者非法执行任意对象代码的风险。

（1）通过密码保护设置，启动禁止覆盖程序

系列	型号	对象版本
可编程控制器 SYSMAC CS 系列	CS1G/H-CPU□□H	单元版本 2.0 及以上
	CS1D-CPU□□S	单元版本 2.0 及以上
SYSMAC CJ 系列	CJ2H-CPU6□-EIP CJ2H-CPU6□	所有版本
	CJ2M-CPU□□	所有版本
SYSMAC CP 系列	CP1H-X40D□-□	所有版本

系列	型号	对象版本
	CP1H-XA40D□-□ CP1H-Y20DT-D	
	CP1L-EL20D□-□ CP1L-EM□□D□-□ CP1L-L□□D□-□ CP1L-M□□D□-□	所有版本

相关设置可参阅 CX-Programmer Ver.9.[] Operation Manual（W446-E1）

Extended Protection Passwords (Option).

（2）通过设置 PLC 的指拨开关，禁止改写用户程序

系列	型号	适用版本	手册
可编程控制器 SYSMAC CS 系列	CS1G/H-CPU□□H	所有版本	CS 系列 CPU Unit Programmable Controllers Operation Manual (W339-E1) 6-1 DIP Switch Settings
	CS1D-CPU□□S	所有版本	CS 系列 CS1D Duplex System Operation Manual (W405-E1) 2-4 CPU Units
	CS1D-CPU□□H	所有版本	
SYSMAC CJ 系列	CJ2H-CPU6□-EIP CJ2H-CPU6□	所有版本	CJ 系列 CJ2 CPU Unit User’s Manual (Hardware) (W472-E1) 3-1 CPU Units
	CJ2M-CPU□□	所有版本	
SYSMAC CP 系列	CP1H-X40D□-□ CP1H-XA40D□-□ CP1H-Y20DT-D	所有版本	CP 系列 CP1H CPU Unit Operation Manual (W450-E1) 6-6-2 Write Protection
	CP1L-EL20D□-□ CP1L-EM□□D□-□	所有版本	CP 系列 CP1L-EL/EM CPU Unit Operation Manual （W516-E1） 8-7-2 Write Protection
	CP1L-L□□D□-□ CP1L-M□□D□-□	所有版本	CP 系列 CP1L CPU Unit Operation Manual （W462-E1） 6-7-2 Write Protection

此外，我们也十分建议您采取以下对策措施：

- 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 网络隔（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。

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

■其他

该漏洞及其应对措施建议来源于欧姆龙相关外部机构对外公开的内容：

- JVN：JVNVU#97111518
  欧姆龙的 SYSMAC CS/CJ/CP 系列和 NJ/NX 系列中的多个漏洞
  https://jvn.jp/vu/JVNVU97111518/

- CISA：ICS Advisory (ICSA-22-179-02)
  Omron SYSMAC CS/CJ/CP Series and NJ/NX Series
  https://www.cisa.gov/uscert/ics/advisories/icsa-22-179-02

■更新记录

2022/12/21 创建