可编程控制器 CJ/CS/CP 系列

中绕过用户存储保护功能的漏洞

发布日期：2023 年 03 月 13 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 CJ/CS/CP 系列可编程控制器中，存在“不当访问控制（CWE-284）”的漏洞。攻击者可能会利用该漏洞绕过用户存储（以下简称 UM）的保护机制，使密码失效或写入新密码、或重新写入用户程序的执行代码和功能块的定义。

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
SYSMAC CP 系列	CP2E-E□□D□-□ CP2E-S□□D□-□ CP2E-N□□D□-□	所有版本
	CP1H-X40D□-□ CP1H-XA40D□-□ CP1H-Y20DT-D	所有版本
	CP1L-EL20D□-□ CP1L-EM□□D□-□ CP1L-L□□D□-□ CP1L-M□□D□-□	所有版本
	CP1E-E□□D□-□ CP1E-NA□□D□-□	所有版本

■漏洞内容

在可编程控制器 CJ/CS/CP 系列中，存在“不当访问控制（CWE-284）”的漏洞。

■漏洞可能造成的威胁

攻击者可能会利用该漏洞绕过 UM 的保护机制，使密码失效或写入新密码、或重新写入用户程序的执行代码和功能块的定义。

■CVSS 评分

不当访问控制（CWE-284）

CVE-2023-0811

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H　基础评分 9.1

■对策方法

使用下面列出的产品时，可采取措施（1）或（2）应对该漏洞。

(1)启用对 UM 写入进行设定的硬件开关（CPU 单元正面的拨动开关）。

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 Hardware User's Manual (Cat. No. W472) "3-1 CPU Units"
	CJ2M-CPU□□	所有版本	
	CJ1G-CPU□□P	所有版本	参见 CJ 系列 Programmable Controllers Operation Manual (Cat. No. W393) "6-1 Overview"
SYSMAC CS 系列	CS1H-CPU□□H CS1G-CPU□□H	所有版本	参见 CS 系列 Programmable Controllers Operation

			Manual (Cat. No. W339) “6-1 DIP Switch Settings”
	CS1D-CPU□□HA CS1D-CPU□□H	所有版本	参见 CS 系列 CS1D Duplex System Operation Manual (Cat. No. W405) “2-4 CPU Units ”
	CS1D-CPU□□SA CS1D-CPU□□S	所有版本	
	CS1D-CPU□□P	所有版本	
SYSMAC CP 系列	CP1H-X40D□-□ CP1H-XA40D□-□ CP1H-Y20DT-D	所有版本	参见 CP 系列 CP1H CPU Unit Operation Manual (Cat. No. W450) “6-6-2 Write Protection”
	CP1L-EL20D□-□ CP1L-EM□□D□-□	所有版本	参见 CP 系列 CP1L-EL/EM CPU Unit Operation Manual (Cat. No. W516) “8-7-2 Write Protection”
	CP1L-L□□D□-□ CP1L-M□□D□-□	所有版本	参见 CP 系列 CP1L CPU Unit Operation Manual (Cat. No. W462) “6-7-2 Write Protection”

(2)设置“基于密码的读取保护功能”和“禁止覆盖程序（可选）”。

系列	型号	对象版本
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	单元 Ver.2.0 或更高版本

SYSMAC CS 系列	CS1H-CPU□□H CS1G-CPU□□H	单元 Ver.2.0 或更高版本
	CS1D-CPU□□SA CS1D-CPU□□S	所有版本
SYSMAC CP 系列	CP1H-X40D□-□ CP1H-XA40D□-□ CP1H-Y20DT-D	所有版本
	CP1L-EL20D□-□ CP1L-EM□□D□-□ CP1L-L□□D□-□ CP1L-M□□D□-□	所有版本

关于该功能，请参见 CX-Programmer Ver.9.□Operation Manual（Cat. No. W446）

（Applying a Password to the PLC Programs）

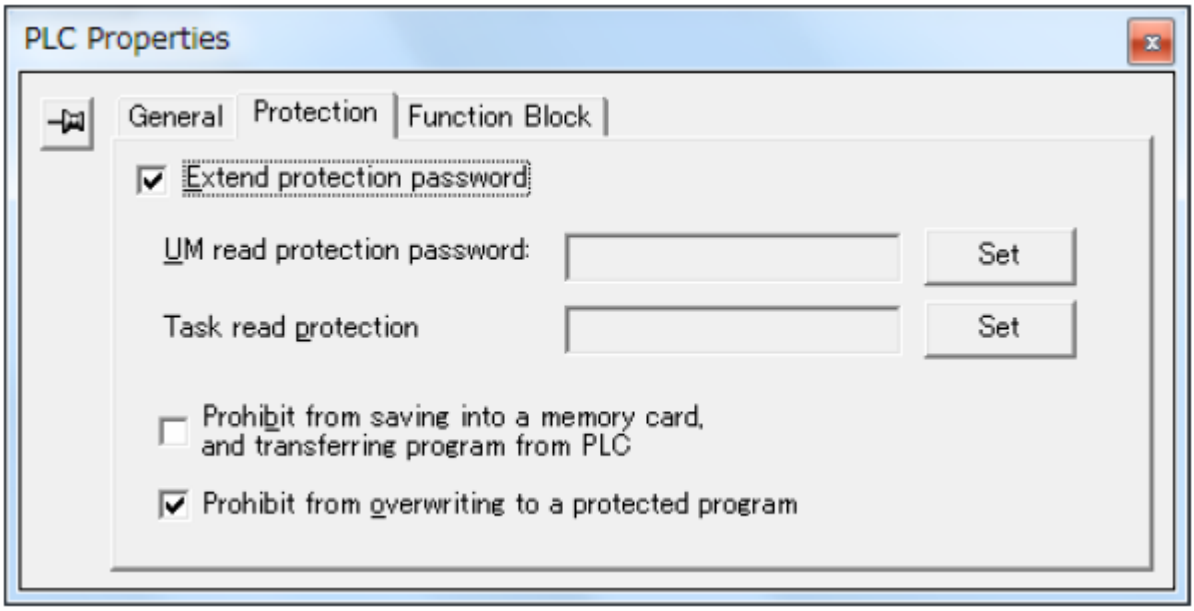
遵循以下步骤进行设定。

1. 【PLC Properties】中注册密码。

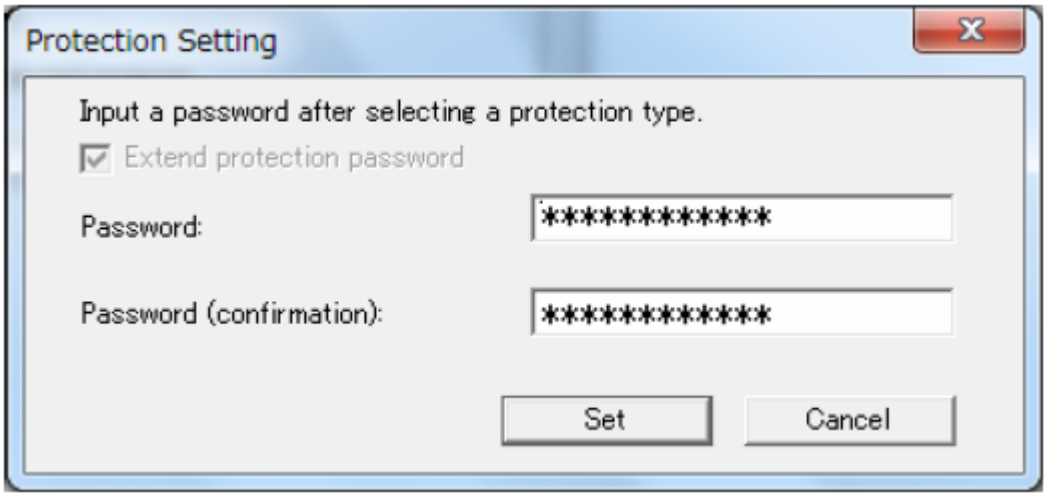
(1) 勾选“禁止覆盖受保护的程序”。

(2) 选择 UM 读取保护密码右侧的“Set”按钮。

使用支持扩展型读取保护功能的 PLC 和 9.6 或更高版本的 CX-Programmer 时，可将 UM 读取保护密码的最大位数扩展至 16 位。建议勾选“扩展保护密码”（“Extend production password”）并设定一个强度更高的密码。



(3) 在“保护设定（Protection Setting）”对话框中输入密码并选择“Set”按钮。



(4) 关闭“PLC Properties”对话框。

2. 在线连接 PLC 并施加读取保护。

■减轻措施/解决方法

如果无法采取上述对策，建议采取以下减轻措施。

1.防止未经授权的访问

使用下面列出的产品及版本时，可采取对策 (1) 或 (2)，从而减轻攻击者经由网络进行攻击的风险。

(1)启用 FINS 写入保护功能

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 Ver.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 Ver.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)"

SYSMAC CP 系列	CP1H-X40D□-□ CP1H-XA40D□-□ CP1H-Y20DT-D	所有版本	参见 CP 系列 CP1H CPU Unit Operation Manual (Cat. No. W450) “6-6-2 Write Protection”

(2)基于 IP 地址进行保护

系列	型号	对象版本	手册
可编程控制器 SYSMAC CP 系列	CP2E-N□□D□-□	所有版本	参见 CP 系列 CP2E CPU Unit Software User's Manual (Cat. No. W614) “15-4-4 PLC Setup ”

此外，还推荐采取以下对策。

1.防止非法访问

・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。

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

■谢辞

Dragos 公司的 Sam Hanson 先生通过 CISA（Cybersecurity & Infrastructure Security Agency）报告了这一漏洞。在此对发现并报告这一漏洞的 Sam Hanson 先生表示感谢。

■更新记录

2023/03/13 创建