可程式控制器CJ/CS/CP系列中

繞過使用者儲存保護功能的漏洞

發佈日期：2023年3月13日

台灣歐姆龍股份有限公司

■概要

歐姆龍一直致力於在工業自動化領域為客戶提供安全、可靠、高品質的產品與解決方案，這是我們立足行業，持續助推客戶業務增長，為客戶創造價值的根基。

近期，我們發現在CJ/CS/CP系列可程式控制器中，存在“不當存取控制（CWE-284）”的漏洞。攻擊者可能會利用該漏洞繞過使用者儲存（以下簡稱UM）的保護機制，使密碼失效或寫入新密碼、或重新寫入使用者程式的執行代碼和功能塊的定義。

為了使您的安全得到有效保護，我們第一時間採取行動，排查受該漏洞影響的產品和版本，並推出相應對策、以及減輕措施/解決方法。您可以通過下述推薦的減輕措施/解決方法，實現將該漏洞的惡意利用風險降至最低。

■受影響產品

受本漏洞影響的產品型號及版本如下所示。

系列	型號	適用版本
可编程控制器 SYSMAC CJ系列 CJ2H CPU單元	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

■漏洞內容

在可程式控制器CJ/CS/CP系列中，存在“不當存取控制（CWE-284）”的漏洞。

■漏洞可能造成的威脅

攻擊者可能會利用該漏洞繞過UM的保護機制，使密碼失效或寫入新密碼、或重新寫入使用者程序的執行代碼和功能塊的定義。

■CVSS 評分

不當存取控制（CWE-284）

漏洞：CVE-2023-0811

CVSS：3.1/AV：N/AC：L/PR：N/UI：N/S：U/C：N/I：H/A：H　基礎評分 9.1

■對策方法

使用下面列出的產品時，可採取措施（1）或（2）應對該漏洞。

（1）啟用對UM寫入進行設定的硬體開關（CPU單元正面的撥動開關）。

系列	型號	對策版本	手冊
可编程控制器 SYSMAC CJ系列	CJ2H-CPU6□-EIP CJ2H-CPU6□	所有版本	請參閱《CJ系列 CJ2 CPU單元用戶手冊硬體篇（SBCA-349）》中的第3-1節「CPU單元」。
	CJ2M-CPU□□	所有版本	
	CJ1G-CPU□□P	所有版本	請參閱《CJ系列用戶手冊設定篇（SBCA-312）》中的第6-1節「Dip開關的設定」。

SYSMAC CS系列	CS1H-CPU□□H CS1G-CPU□□H	所有版本	請參閱《CS系列 CPU單元 用戶手冊 設定篇（SBCA-301）》中的第6-1節「Dip開關的設定」。
	CS1D-CPU□□HA CS1D-CPU□□H	所有版本	請參閱《CS系列 CS1D 雙重化系統 用戶手冊 設定篇（SBCA-318）》中的第2-4節「CPU單元」。
	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	請參閱《CP系列 CP1H CPU單元 用戶手冊（SBCA-340）》中的第6-6-2節「寫入保護」。
	CP1L-EL20D□-□ CP1L-EM□□D□-□	所有版本	請參閱《CP系列 CP1L-EL/EM CPU單元 用戶手冊（SBCA-406）》中的第8-7-2節「寫入保護」。
	CP1L-L□□D□-□ CP1L-M□□D□-□	所有版本	請參閱《CP系列 CP1L CPU單元 用戶手冊（SBCA-345）》中的第6-7-2節「寫入保護」。

（2）設定「密碼讀取保護功能」，並啟用「禁止覆蓋程序（選項）」。

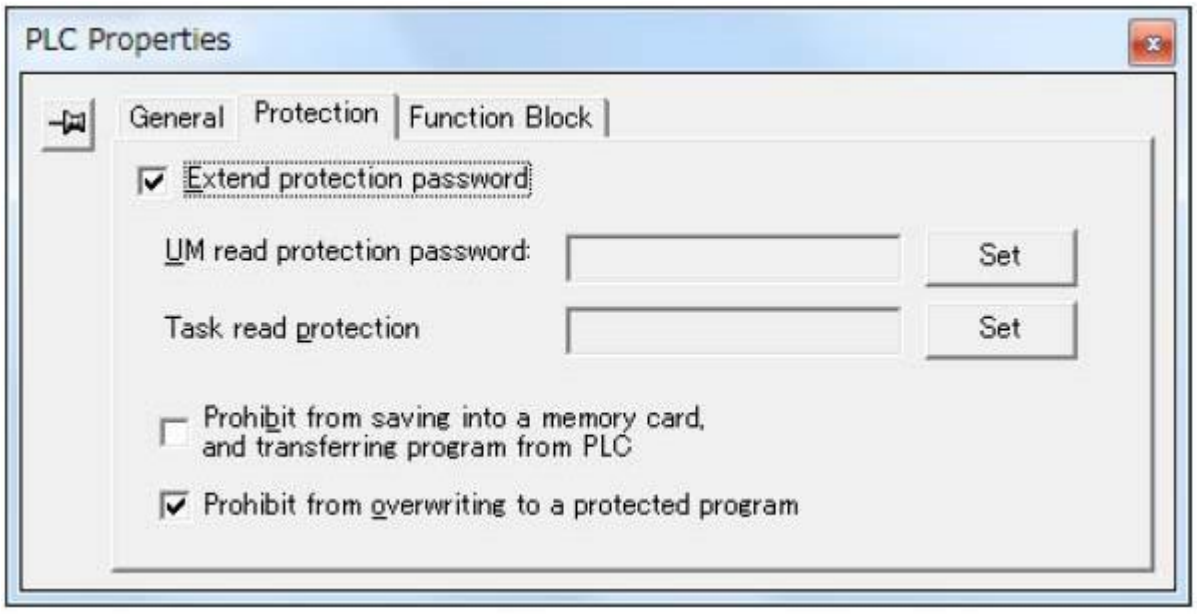
系列	型號	對象版本
可编程控制器 SYSMAC CJ系列	CJ2H-CPU6□-EIP CJ2H-CPU6□	所有版本
	CJ2M-CPU□□	所有版本
	CJ1G-CPU□□P	單元版本 2.0或更高版本
SYSMAC CS系列	CS1H-CPU□□H CS1G-CPU□□H	單元版本 2.0或更高版本
	CS1D-CPU□□SA CS1D-CPU□□S	所有版本
SYSMAC CP系列	CP1H-X40D□-□ CP1H-XA40D□-□ CP1H-Y20DT-D	所有版本

	CP1L-EL20D□-□ CP1L-EM□□D□-□ CP1L-L□□D□-□ CP1L-M□□D□-□	所有版本

有關該功能，請參考《CX-Programmer Ver.9.□ 操作手冊（SBCA-337）》中的第9-15節「密碼讀取保護」。您可以根據手冊中的步驟進行設定。

1. 在 PLC 的屬性中，註冊密碼。
   (1) 勾選「禁止覆蓋保護中的程序」。
   (2) 選擇 UM 讀取保護密碼右側的「設定」按鈕。如果使用支援擴展型讀取保護功能的 PLC 和 CX-Programmer 9.6 或更高版本，UM 讀取保護密碼的最大字數可以擴展到 16 位，建議勾選「擴展保護密碼」，並設定更強的密碼。

支援擴展型讀取保護功能的 PLC 型號和版本，請參考《CX-Programmer Ver.9.□ 操作手冊（SBCA-337）》中的第9-15節「密碼讀取保護 ●擴展保護密碼（選項）」。該節提供了詳細的資訊和設定步驟。



（3） 在「保護設定（Protection Setting）」對話框中輸入密碼並選擇“Set”按鈕。

（4） 關閉「PLC Properties」對話框。

在線連接後，對 PLC 進行讀取保護設置。

■減輕措施/解決方法

如果無法採取上述對策，建議採取以下減輕措施。

1.防止未經授權的存取

使用下面列出的產品及版本時，可採取對策（1）或（2），從而減輕攻擊者經由網路進行攻擊的風險。

（1） 啟用FINS寫入保護功能

系列	型號	對策版本	手冊
可编程控制器 SYSMAC CJ系列	CJ2H-CPU6□-EIP CJ2H-CPU6□	所有版本	請參閱《CJ系列 CJ2 CPU 單元用戶手冊 軟體篇（SBCA-350）》中的第9-3-8節「FINS保護」部分，瞭解如何設置FINS保護功能。
	CJ2M-CPU□□	所有版本	
	CJ1G-CPU□□P	單元版本 2.0以上	請參閱《CJ系列使用者手冊 設定篇（SBCA-312)》的第1-7-3節，瞭解如何通過網路對CPU單元進行

			FINS寫入保護功能的設定。
SYSMAC CS系列	CS1H-CPU□□H CS1G-CPU□□H	單元版本 2.0以上	請參閱《CS系列 CPU單元 用戶手冊 設定篇（SBCA-301）》中的第1-7-3節「透過網絡對CPU單元的FINS寫入保護功能」。
	CS1D-CPU□□SA CS1D-CPU□□S	所有版本	請參閱《CS系列 CS1D 雙重化系統 用戶手冊 設定篇（SBCA-318）》中的第6-2-9節「FINS保護標籤（僅適用於CPU單獨系統）」。
SYSMAC CP系列	CP1H-X40D□-□ CP1H-XA40D□-□ CP1H-Y20DT-D	所有版本	請參閱《CP系列 CP1H CPU單元 用戶手冊（SBCA-340）》中的第6-6-2節「寫入保護」。

(2) 進行基於 IP 位址的保護設置。

系列	型號	對策版本	手冊
可编程控制器 SYSMAC CP系列	CP2E-N□□D□-□	所有版本	請參閱《CP系列 CP2E CPU單元 用戶手冊 軟體篇（SBCA-478）》中的第15-4-4節「PLC系統設定」。

此外，還推薦採取以下對策。

1.防止非法存取

- 最大限度地減少控制系統或設備的網路連接，禁止不受信任的設備存取。
- 透過部署防火牆來隔離 IT 網路（斷開未使用的通信埠、限制通信主機、限制對 FINS 埠（9600）的存取）。
- 需要遠端存取控制系統或設備時，使用虛擬專用網路（VPN）。
- 使用高強度密碼並定期修改。
- 引入物理控制，確保僅授權人員可存取控制系統和設備。
- 在控制系統或設備中使用 USB 記憶體等外部儲存設備時，事先進行病毒掃描。
- 在遠端存取控制系統或設備時進行多重要素驗證。

2.防病毒保護

在連接控制系統的電腦上安裝最新版本的企業級防毒軟體，並定期維護。

3. 數據輸入/輸出保護

確認備份和範圍檢查等設置的合理性，以防止對控制系統和設備的輸入/輸出數據進行意外修改。

4.恢復丟失的資料

定期對設置數據進行備份和維護，以防數據丟失。

■諮詢方式

如您在採取減輕措施/解決方案時遇到問題，可以透過以下方式聯繫歐姆龍營業據點或經銷商：

https://www.ia.omron.com/global_network/index.html

■謝辭

Dragos公司的Sam Hanson先生通過CISA（Cybersecurity & Infrastructure Security Agency）報告了這一漏洞。在此對發現並報告此漏洞的Sam Hanson先生表示感謝。

■更新記錄

2023年3月13日 建立