可程式控制器CS/CJ系列中

文件系統缺乏驗證的漏洞

發佈日期：2023年4月17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，我們發現在可程式控制器 CS/CJ 系列中，存在“關鍵功能缺乏驗證（CWE-306）”的漏洞。 攻擊者可能會利用該漏洞，無需認證即可存取 CPU 單元提供的文件系統（儲存卡或 EM 檔記憶體），竊取機密資訊。

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
可程式控制器 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

■漏洞內容

在可程式控制器CS/CJ系列中，存在“關鍵功能缺乏驗證（CWE-306）”的漏洞。

■漏洞可能造成的威脅

攻擊者可能會利用該漏洞，無需認證即可存取CPU單元提供的文件系統（儲存卡或EM檔記憶體），竊取機密資訊。

■CVSS 評分

關鍵功能缺乏驗證（CWE-306）

CVE-2022-45794漏洞

CVSS：3.1/AV：N/AC：L/PR：N/UI：N/S：U/C：H/I：N/A：N 基礎評分 7.5

■減輕措施/解決方法

為了將這些漏洞的惡意利用風險降至最低，我們強烈建議您採取以下減輕措施。

1.防止未經授權的存取

・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。

・通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。

此外，使用如下所示的產品及版本時，也可透過啟用FINS寫保護功能，對寫入採取措施。

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）」

2. 防毒保護

為連接到控制系統的電腦安裝並維護最新的商用級防毒軟體。

3. 資料輸入輸出保護

通過備份和範圍檢查等方式，確保控制系統和設備的輸入輸出數據不被意外修改。

4. 資料遺失復原

定期備份並維護設置數據，以防止資料遺失。

■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

■更新記錄

2023年4月17日 建立