可程式控制器CS/CJ/CP系列FINS協定

存在交互頻率控制不當漏洞

發佈日期：2023年9月19日
更新日期：2023年11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，我們發現可程式控制器 CS/CJ/CP 系列 FINS 協定存在交互頻率控制不當（CWE-799）漏洞。攻擊者可利用本漏洞解除受密碼保護的記憶體區域的保護，進而不經授權獲取相應控制器產品中的資訊。

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。

此外，為了確保您安心使用本產品，我們還為受該漏洞影響的產品準備了安全增強的對策版本。您可在下文“對策方法”處查找對應的對策版本。

■受影響產品

受本漏洞影響的產品型號及版本如下所示。

產品名稱	型號	適用版本
可編程控制器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
可編程控制器CS系列	CS1H-CPU□□H CS1G-CPU□□H	Ver.4.0以下
	CS1D-CPU□□H CS1D-CPU□□P	Ver.1.3以下
	CS1D-CPU□□S	Ver2.0以下
可編程控制器CP系列	CP1E-E	Ver.1.2以下
	CP1E-N	

請參閱以下手冊以確認目標產品的版本。

- CJ系列 CJ2 CPU單元 用戶手冊 硬體篇（SBCA-349）
- CJ系列 CPU單元 用戶手冊 設定篇（SBCA-312）
- CS系列 CPU單元 用戶手冊 設定篇（SBCA-301）
- CS系列 CS1D雙工系統 用戶手冊 設定篇（SBCA-318）
- CP系列 CP1E CPU單元 用戶手冊 軟體篇（SBCA-354）

請參閱上述手冊中的「CPU單元的單元版本」。

■漏洞內容

可程式控制器CS/CJ/CP系列FINS協定存在交互頻率控制不當（CWE-799）漏洞。 攻擊者可利用本漏洞非法存取該產品並進行操作。

■漏洞可能造成的威脅

攻擊者可通過FINS協議連續快速的多次調出「解除記憶體區域保護」，以解除受密碼保護的記憶體區域的保護，進而不經授權獲取相應控制器產品中的資訊。

■CVSS 評分

互動頻率控制不當（CWE-799）

漏洞：CVE-2022-45790

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，並定期進行維護。

2. 防止未經授權的存取

   建議採取以下措施：

   - 最大限度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
   - 通過部署防火牆隔離 IT 網路（斷開未使用的通訊端口、限制通訊主機）
   - 需要遠程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更換
   - 引入實體控制，確保只有授權人員才能存取控制系統和設備
   - 在控制系統或設備中使用 USB 儲存器等外部儲存設備時，先進行病毒掃描
   - 遠程存取控制系統或設備時，實施多重驗證

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. 恢復丟失的數據

   定期對設置數據進行備份和維護，以防數據丟失。

■對策方法

可將各產品更新至對策版本以應對漏洞。

各產品的對策版本與發佈日期見下表。

產品名稱	型號	對策版本	對策版本 推出時間
可編程控制器CJ系列	CJ2H-CPU□□(-EIP)	Ver.1.5以上	已於2016年提供
	CJ2M-CPU□□	Ver.2.1以上	
	CJ1G-CPU□□P	Ver.4.1以上	
可編程控制器CS系列	CS1H-CPU□□H CS1G-CPU□□H	Ver.4.1以上	
	CS1D-CPU□□H CS1D-CPU□□P	Ver.1.4以上	
	CS1D-CPU□□S	Ver2.1以上	
可編程控制器CP系列	CP1E-E CP1E-N	Ver.1.3以上	

上述對策版本的獲取途徑及更新方法，請諮詢本公司銷售窗口。

■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Reid Wightman先生通過CISA報告了本漏洞。

我們在此感謝發現並報告此漏洞的Reid Wightman先生。

■更新記錄

2023年9月19日創建

2023年11月13日 修正對策品的獲取方法