

## CJ系列CJ2 CPU單元內建的EtherNet/IP™埠、 以及CS/CJ系列EtherNet/IP™單元停止服務 (DoS) 的漏洞

發佈日期：2023年8月1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CJ系列CJ2 CPU單元內置的EtherNet/IP™埠、以及CS/CJ系列EtherNet/IP™單元的通信功能存在對指定類型輸入的驗證不當 (CWE-1287) 的漏洞。攻擊者可透過發送非法數據包，利用該漏洞使相應的單元停止服務 (DoS)。

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。

系列	型號	適用版本
CJ2M CPU單元	CJ2M-CPU3□	內建EtherNet/IP™部的單元版本為V2.18以下
CJ2H CPU單元	CJ2H-CPU6□-EIP	內建EtherNet/IP™部的單元版本為V3.04以下
CS/CJ系列 EtherNet/IP™ 單元	CS1W-EIP21 CJ1W-EIP21	V3.04以下

請參考以下手冊以確認適用產品的版本：

- CJ系列CJ2 CPU單元用戶手冊 硬體篇 (SBCA-349) 請參照上述手冊中的「CJ2 CPU單元的單元版本」
- CS/CJ系列EtherNet/IP™單元用戶手冊 (SBCD-342) 請參照上述手冊中的「關於單元版本」

#### ■ 漏洞內容

CJ系列CJ2 CPU單元內置的EtherNet/IP™埠、以及CS/CJ系列EtherNet/IP™單元的通信功能存在對指定類型輸入的驗證不當（CWE-1287）的漏洞，攻擊者可通過發送非法數據包，使相應的單元停止服務（DoS）。

#### ■ 漏洞可能造成的威脅

攻擊者可利用該漏洞使相應的單元停止服務（DoS）。

#### ■ CVSS 評分

指定類型輸入的驗證不當（CWE-1287）

CVSS：3.1/AV：N/AC：L/PR：N/UI：N/S：U/C：N/I：N/A：H 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。

系列	型號	對策版本	對策版本 推出時間
CJ2M CPU單元	CJ2M-CPU3□	內建 EtherNet/IP™ 部的單元版本 為V2.19以上	2023年6月16日
CJ2H CPU單元	CJ2H-CPU6□-EIP	內建 EtherNet/IP™ 部的單元版本 為V3.05以上	2023年8月1日
CS/CJ系列 EtherNet/IP™ 單元	CS1W-EIP21 CJ1W-EIP21	V3.05以上	2023年8月1日

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](https://www.ia.omron.com/global_network/index.html)

### ■ 更新記錄

2023年8月1日 創建

2023年9月1日 修正對策版本的發佈日期

2023年11月13日 修正對策版本的獲取途徑