NJ/NX 系列機器自動化控制器通訊功能中的違反最低權限漏洞

發布日期: 2025 年 7 月 14 日
台灣歐姆龍股份有限公司

■ 概述

NJ/NX 系列機器自動化控制器與 Sysmac Studio 軟體之間的通訊功能中，存在違反最低權限（CWE-272）漏洞。攻擊者可能會利用此漏洞，對控制器產品進行未經授權的存取，甚至遠端執行未經授權的程式碼。

以下列出受此漏洞影響的產品、版本以及減輕風險的對策與迴避方法。透過執行我們建議的對策與迴避方法，可以將此漏洞被利用的風險降至最低。此外，為了讓客戶更加安心地使用產品，我們已準備了針對本次安全性強化的對策版本。關於各產品的對應版本，請參考本文中的對策方法，並請配合實施相關對策。

■ 受影響產品

受影響產品型號及其版本如下所示。

機械自動化化控制器 NJ 系列

型號	適用版本	Lot number（生產日期）
NJ101-□□□□	Ver.1.67.00 以前	13725 (2025 年 7 月 13 日)以前
NJ301-1□00	Ver.1.67.00 以前	
NJ501-1□00	Ver.1.67.02 以前	
NJ501-1□20	Ver.1.68.01 以前	
NJ501-1340	Ver.1.67.00 以前	
NJ501-4□□□	Ver.1.67.00 以前	
NJ501-5300	Ver.1.67.01 以前	
NJ501-R□00	Ver.1.67.01 以前	
NJ501-R□20	Ver.1.67.00 以前	

如何查看受影響的版本：請參閱附件「產品版本的確認方法」。
有關如何檢查批號的說明，請參閱操作手冊中的「ID Information Indication」。

- NJ-series CPU unit Hardware User’s Manual（W500）

機械自動化化控制器 NX 系列

型號	適用版本	Lot number（生產日期）
NX102-□□□□	Ver.1.68.01 以前	13725 (2025 年 7 月 13 日)以前
NX1P2-□□□□□□	Ver.1.64.09 以前	
NX1P2-□□□□□□1	Ver.1.64.09 以前	
NX502-□□□□	Ver.1.68.01 以前	
NX701-□□□□	Ver.1.35.09 以前	

如何查看受影響的版本：請參閱附件「產品版本的確認方法」。

有關如何檢查批號的說明，請參閱操作手冊中的「ID Information Indication」。

・NX102 CPU Unit User’s Manual (Hardware) (W593)

・NX1P2 CPU Unit User’s Manual (Hardware) (W578)

・NX5 CPU Unit User’s Manual (Hardware) (W629)

・NX7 CPU Unit User’s Manual (Hardware) (W535)

Sysmac Studio 軟體

型號	適用版本
SYSMAC-SE2□□□	全部

請參閱操作手冊中的「Displaying and Registering Licenses」章節，以確認產品版本。

・Sysmac Studio Version 1 Operation Manual (W504)

■ 說明

由於 NJ/NX 系列機器自動化控制器中存在違反最低權限（CWE-272）漏洞，該產品可能遭受未經授權的存取，並可能被遠端執行任意程式碼（RCE，Remote Code Execution）。

■ CWE,CVE,CVSS 評分

違反最低權限（CWE-272）

CVE-2025-1384

CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:L/I:L/A:H 基本值 7.0

■ 對策

將各產品更新至對應的修正版本，並設定為安全通訊版本 2(Secure Communication Version 2)。

1.將產品更新至加強安全性的對應版本

各產品的對應修正版本及其發佈日期，請參見下表。

機械自動化化控制器 NJ 系列

型號	對策版本	Lot number	對策版本提供時間
NJ101-□□□□	Ver.1.69.00 以上	14725 之後	2025 年 7 月 14 日
NJ301-1□00			
NJ501-1□00			
NJ501-1□20			
NJ501-1340			
NJ501-4□□□			
NJ501-5300			
NJ501-R□00			
NJ501-R□20			

上述對策版本的獲取途徑及更新方法，請諮詢本公司營業窗口。

機械自動化化控制器 NX 系列

型號	適用版本	Lot number（生產日期）	對策版本提供時間
NX102-□□□□	Ver.1.69.00 以上	14725 之後	2025 年 7 月 14 日
NX1P2-□□□□□□			
NX1P2-□□□□□□1			
NX502-□□□□			
NX701-□□□□	Ver.1.36.00 以上		

述對策版本的獲取途徑及更新方法，請諮詢本公司營業窗口。

Sysmac Studio 軟體

型號	適用版本	對策版本提供時間
SYSMAC-SE2□□□	Ver.1.69.00 以上	2025 年 7 月 14 日

您可以使用已安裝的 OMRON 自動化軟體自動更新工具更新至最新版本。

2. 設定安全通訊版本 2

首次使用 Sysmac Studio 線上設定安全通訊版本，或從安全通訊設定畫面設定。

有關如何設定安全通訊版本，請參閱操作手冊 Sysmac Studio Version 1 Operation Manual (W504)

■ 缓解措施和保護方法

為了將這些風險降至最低，歐姆龍建議客戶採取下列緩解措施。

1. 使用安全通信功能

   安全通信功能可防止數據被第三方竊聽或篡改。安全通信功能可用於以下 CPU 模組版本。

   - NJ 系列、NX102、NX1P2 CPU 模組：Ver.1.49 或更高版本
   - NX701 CPU 模組：Ver.1.29 或更高版本
   - NX502 CPU 模組：Ver.1.60 或更高版本

2. 防毒保護

   為保護任何可以存取控制系統的 PC 免受惡意軟體的侵害，請確保安裝和維護最新的商業級防毒軟體。

3. 採取安全措施，防止未授權存取

   - 盡量減少控制系統和設備連接開放網路，以防不信任裝置登入。
   - 使用防火墙（關閉未使用的通訊埠，限制通訊主機），將其與 IT 網路隔離。
   - 使用虛擬專用網路（VPN）進行遠端連接控制系統及設備。
   - 使用高強度密码並增加修改頻率。
   - 安裝實物控制，确保僅授權人員可連結控制系統和設備。
   - 在將任何 USB 隨身碟或類似裝置連接到系統和裝置之前，請先掃描病毒以確保其安全。
   - 強化對遠端連接控制系統和設備的多重身分驗證。

4. 資料輸入和輸出保護

   利用備份和範圍檢查等驗證處理措施，以防控制系統和設備輸入/輸出數據被修改。

5. 資料復原

   定期進行數據備份和維護，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

■致謝

微軟 CPS 研究團隊的 Tamir Ariel 報告了這個漏洞。
感謝 Tamir Ariel 發現並報告此漏洞。

■更新紀錄

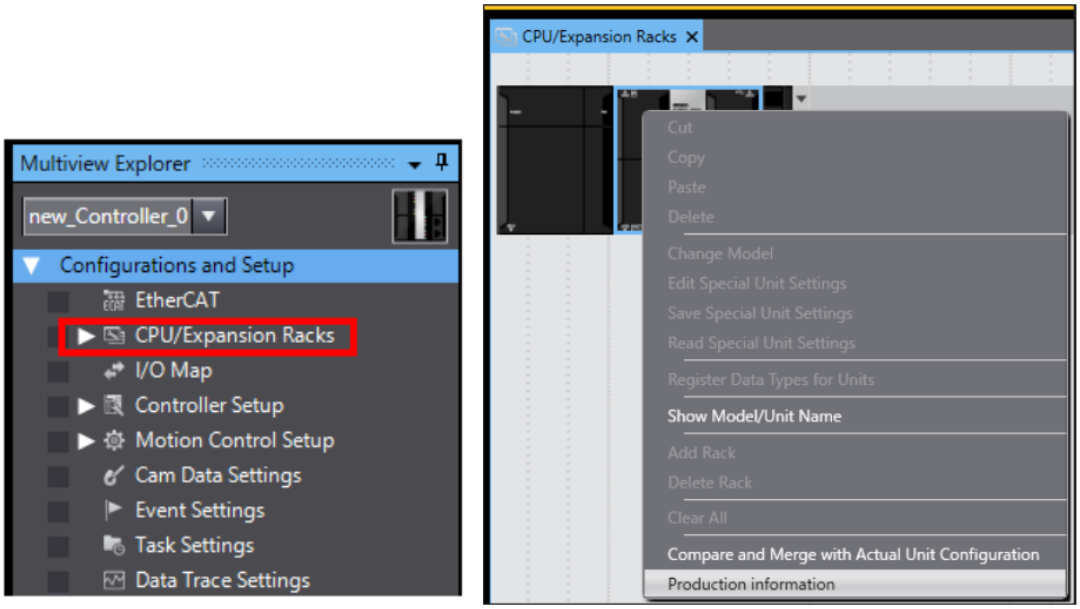
-2025 年 7 月 14 日 最新版本

附錄—產品版本的確認方法

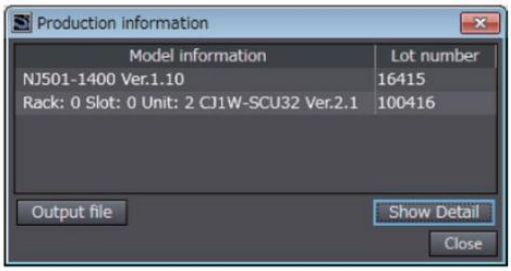
確認產品版本的方法因產品系列而異。

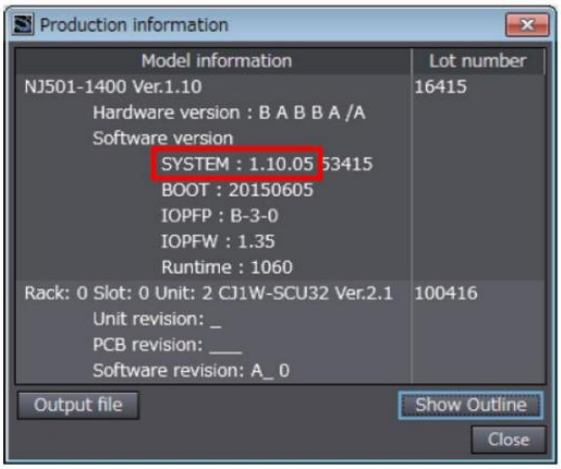
NJ 系列的確認方法

在 Sysmac Studio 的 Multi View Explorer 中按兩下[配置/設置] → [CPU/擴展機 架]。右鍵單擊單元編輯器中的空白字段，然後選擇[顯示產品資訊]。



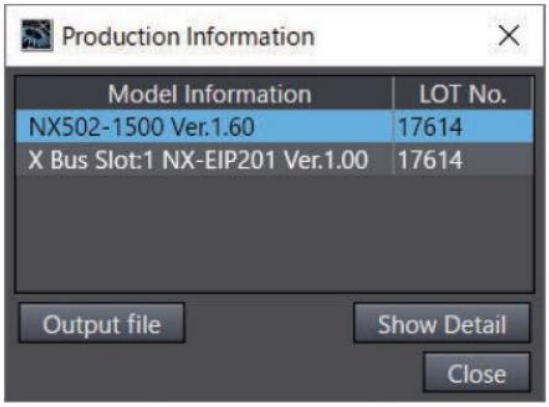
選擇[產品資訊]→[詳細顯示]。下圖顯示 Ver.1.10.05





NX 系列的確認方法

在 Sysmac Studio 的 Multi View Explorer 中右鍵單擊[配置/設置]的[CPU/擴展機架]的[CPU 機架]，然後選擇[顯示產品資訊]。將顯示[產品資訊]對話框。。



在[產品資訊]對話框的右下角選擇[簡單顯示]或[詳細顯示]。切換[產品資訊]的簡單顯示和詳細顯示。下圖顯示 NX502-1500 的 Ver.1.60.02 和 NX-EIP201 的 Ver.1.00.00。