機械自動化控制器 NJ/NX 系列存在路徑遍歷漏洞

發佈日期：2024 年 3 月 7 日

最新更新時間：2024 年 5 月 27 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，我們發現機械自動化控制器 NJ/NX 系列存在路徑遍歷（CWE-22）漏洞。攻擊者可利用本漏洞獲得對控制器產品未經授權的存取、遠端執行代碼。

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

受此漏洞影響的產品型號及版本如下所示。

NJ 系列機械自動化控制器

型號	適用版本	批號（生產日期）
NJ101-□□□□	Ver.1.64.03 以下	25424（2024 年 4 月 25 日前）
NJ301-□□□□	Ver.1.64.00 以下	
NJ501-1□0□	Ver.1.64.03 以下	
NJ501-1□2□	Ver.1.64.00 以下	
NJ501-1340	Ver.1.64.00 以下	
NJ501-4□□□	Ver.1.64.00 以下	
NJ501-5300	Ver.1.64.00 以下	
NJ501-R□□□	Ver.1.64.00 以下	

請參考“附件-產品版本的確認方法”來確認適用版本。

請參考相應手冊的“識別信息顯示”來確認批號。

- NJ 系列 CPU 單元 使用者手冊 硬體篇（SBCA-CN5-466）

機械自動化控制器 NX 系列

型號	適用版本	批號（生產日期）
NX102-□□□□	Ver.1.64.00 以下	25424 之前（2024 年 4 月 25 日前）
NX1P2-□□□□□□	Ver.1.64.00 以下	
NX1P2-□□□□□□1	Ver.1.64.00 以下	
NX502-□□□□	Ver.1.65.01 以下	
NX701-□□□□	Ver.1.35.00 以下	
NX-EIP201	Ver.1.00.01 以下	

請參考“附件-產品版本的確認方法”來確認適用版本。

請參考相應手冊的“識別信息顯示”來確認批號。

- NX 系列 NX102 CPU 單元 用戶手冊 硬體篇（SBCA-CN5-462）
- NX 系列 NX1P2 CPU 單元 用戶手冊 硬體篇（SBCA-CN5-448）
- NX 系列 NX5 CPU 單元 用戶手冊 硬體篇（SBCA-CN5-497）
- NX 系列 NX7 CPU 單元 用戶手冊 硬體篇（SBCA-CN5-418）
- NX 系列 NX-EIP201 EtherNet/IPTM 單元 用戶手冊（SBCA-CN5-382）

■ 漏洞內容

機械自動化控制器 NJ/NX 系列存在路徑遍歷（CWE-22）漏洞，攻擊者可利用本漏洞得對控制器產品，未經授權的存取、遠端執行代碼。

■ CVSS 評分

路徑遍歷（CWE-22）

CVE-2024-27121 漏洞

CVSS：3.1/AV：N/AC：L/PR：H/UI：N/S：U/C：H/I：H/A：H 基礎評分 7.2

■ 對策方法

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。

機械自動化控制器 NJ 系列

型號	對策版本	批號(對策版本推出時間)
NJ101-□□□□	Ver.1.64.04 以上	26424（2024 年 4 月 26 日）之後
NJ301-□□□□	Ver.1.64.04 以上	
NJ501-1□0□	Ver.1.64.04 以上	
NJ501-1□2□	Ver.1.64.04 以上	
NJ501-1340	Ver.1.64.04 以上	
NJ501-4□□□	Ver.1.64.04 以上	
NJ501-5300	Ver.1.64.04 以上	
NJ501-R□□□	Ver.1.64.04 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。

機械自動化控制器 NX 系列

型號	對策版本	批號(對策版本推出時間)
NX102-□□□□	Ver.1.64.04 以上	26424（2024 年 4 月 26 日）之後
NX1P2-□□□□□□	Ver.1.64.04 以上	
NX1P2-□□□□□□1	Ver.1.64.04 以上	
NX502-□□□□	Ver.1.66.01 以上	
NX701-□□□□	Ver.1.35.04 以上	
NX-EIP201	Ver.1.01.00 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。

■減輕措施/解決方法

為了實現將這些漏洞的惡意利用風險降至最低，我們十分建議您採取以下減輕措施。

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 單元的單元版本。

   - NJ 系列、NX102、NX1P2 CPU 單元：Ver.1.49 以上
   - NX701 CPU 單元：Ver.1.29 以上
   - NX502 CPU 單元：Ver.1.60 以上
   - NX-EIP201：Ver.1.00 以上

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殺毒軟體，並定期維護。

3. 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

4. 資料輸入/輸出保護

   確認備份和範圍檢查等設置的合理性，以防對控制系統和設備的輸入/輸出數據的意外修改

5. 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

■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

Microsoft 公司 CPS Research Team 的 Tamir Ariel 先生報告了本漏洞。

Dragos 公司 Principle Vulnerability Analyst 的 Logan Carpenter 先生報告了本漏洞。

我們在此感謝發現並報告此漏洞的 Tamir Ariel 先生和 Logan Carpenter 先生。

■更新記錄

2024 年 3 月 7 日創建

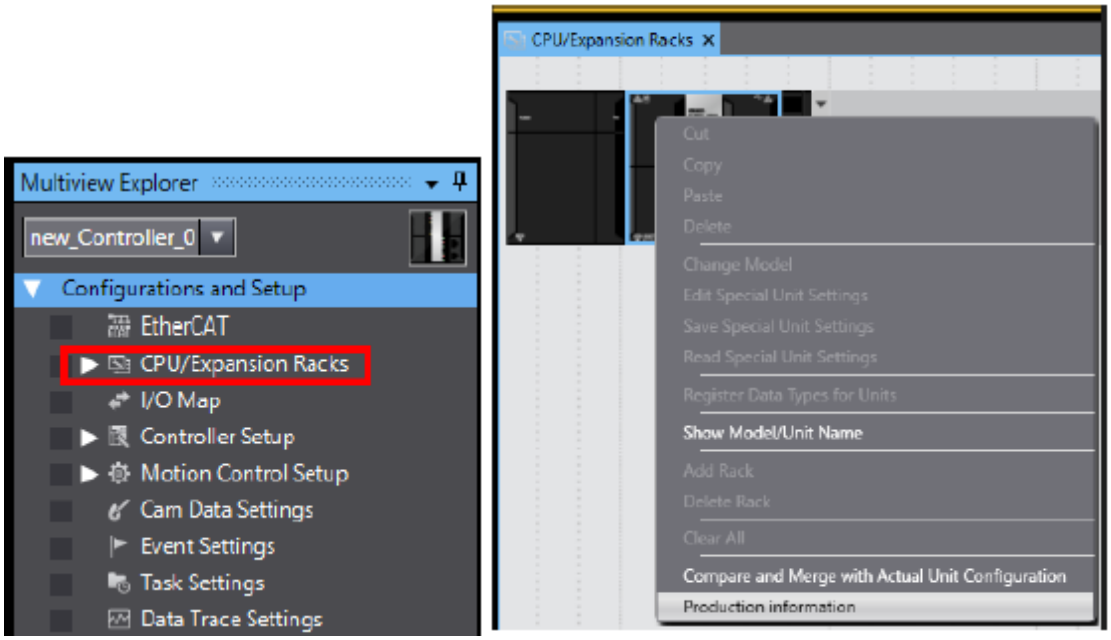
2024 年 5 月 27 日修正對象產品、對策版本的批號

附件-產品版本的確認方法

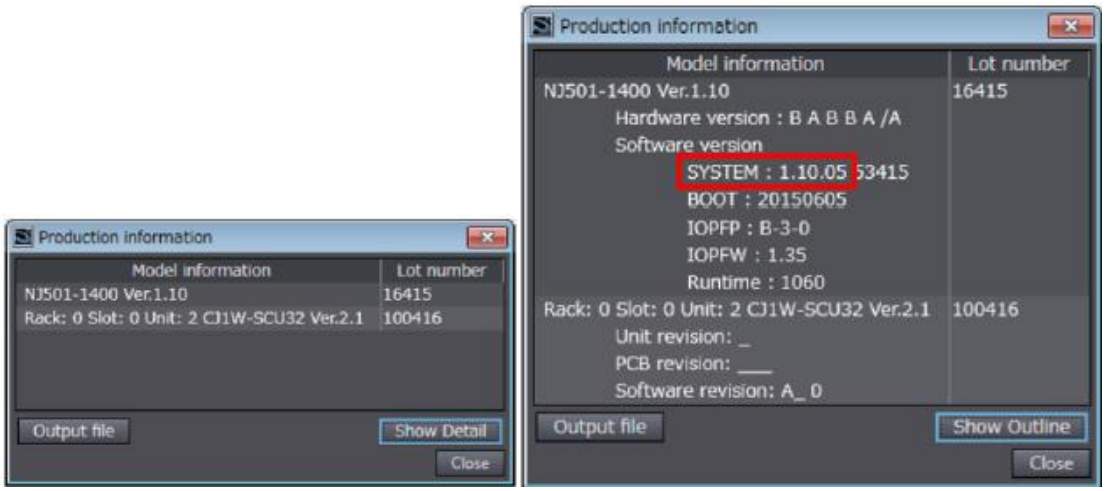
確認產品版本的方法因產品系列而異。

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]。

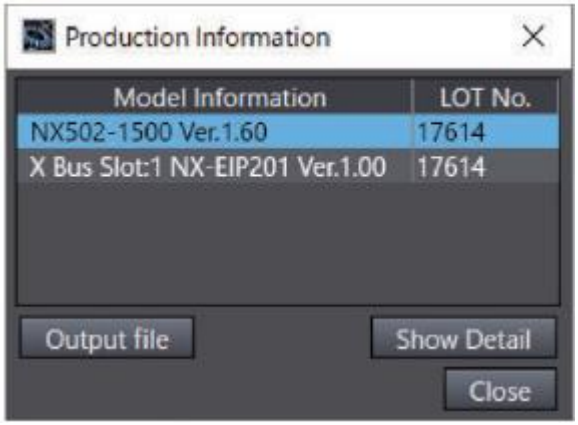


選擇[產品資訊]→[詳細顯示]。下圖顯示 Ver.1.10.05。



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。