機械自動化控制器 NJ/NX 系列的 OpenSSL 引起的多個漏洞

發布日期：2024 年 5 月 27 日

台灣歐姆龍股份有限公司

■ 概述

歐姆龍一直致力於在工業自動化領域為客戶提供安全、可靠且高質量的產品與解決方案。這是我們立足行業，持續推動客戶業務增長並為客戶創造價值的基石。

近期，我們發現機械自動化控制器 NJ/NX 系列使用的 OpenSSL 庫中存在明顯不一致（CWE-203）、雙重釋放（CWE-415）和釋放後使用（CWE-416）的漏洞。攻擊者可以利用這些漏洞導致控制器的產品信息洩露或服務中斷（DoS）。

為了保護您的安全，我們第一時間採取了行動，排查受影響的產品和版本，並推出相應的對策與減輕措施/解決方案。您可以通過以下推薦的減輕措施/解決方案來最大限度地減少這些漏洞被惡意利用的風險。

此外，為確保客戶安心使用我們的產品，我們還為每個產品，提供了安全強化對策。相關對策見下文，請根據所需實施相應的對策。

■ 受影響產品

受影響產品及其版本如下所示。

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 之前（2024 年 4 月 25 日前）
NJ301-□□□□	Ver.1.64.00 以下	25424 之前（2024 年 4 月 25 日前）
NJ501-1□0□	Ver.1.64.03 以下	25424 之前（2024 年 4 月 25 日前）
NJ501-1□2□	Ver.1.64.00 以下	25424 之前（2024 年 4 月 25 日前）
NJ501-1340	Ver.1.64.00 以下	25424 之前（2024 年 4 月 25 日前）
NJ501-4□□□	Ver.1.64.00 以下	25424 之前（2024 年 4 月 25 日前）
NJ501-5300	Ver.1.64.00 以下	25424 之前（2024 年 4 月 25 日前）
NJ501-R□□□	Ver.1.64.00 以下	25424 之前（2024 年 4 月 25 日前）

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 單元用戶手冊（SBCA-CN5-466）

NX 系列機械自動化控制器

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	25424 之前（2024 年 4 月 25 日前）
NX1P2-□□□□□□1	Ver.1.64.00 以下	25424 之前（2024 年 4 月 25 日前）
NX502-□□□□	Ver.1.65.01 以下	25424 之前（2024 年 4 月 25 日前）
NX701-□□□□	Ver.1.35.00 以下	25424 之前（2024 年 4 月 25 日前）
NX-EIP201	Ver.1.00.01 以下	25424 之前（2024 年 4 月 25 日前）

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（SBCA-CN5-462）
- NX 系列 NX1P2 CPU 單元用戶手冊（SBCA-CN5-448）
- NX 系列 NX5 CPU 單元用戶手冊（SBCA-CN5-497）
- NX 系列 NX7 CPU 單元用戶手冊（SBCA-CN5-418）

■ 漏洞內容

NJ/NX 系列使用的 OpenSSL 庫存在以下漏洞，攻擊者可利用這些漏洞導致控制器產品信息洩露或服務中斷（DoS）。

■ CVSS 評分

(1)明顯不一致（CWE-203）

CVE-2022-4304

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N 基礎評分：5.9

(2)雙重釋放（CWE-415）

CVE-2022-4450

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

(3)釋放後使用（CWE-416）

CVE-2023-0215

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

■ 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布日期見下表。

NJ 系列機械自動化控制器

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

若需了解如何獲取對策版本和更新方法，請聯繫本公司銷售窗口。

NX 系列機械自動化控制器

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

若需了解如何獲取對策版本和更新方法，請聯繫本公司銷售窗口。

■ 減輕措施/解決方案

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。

■ 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

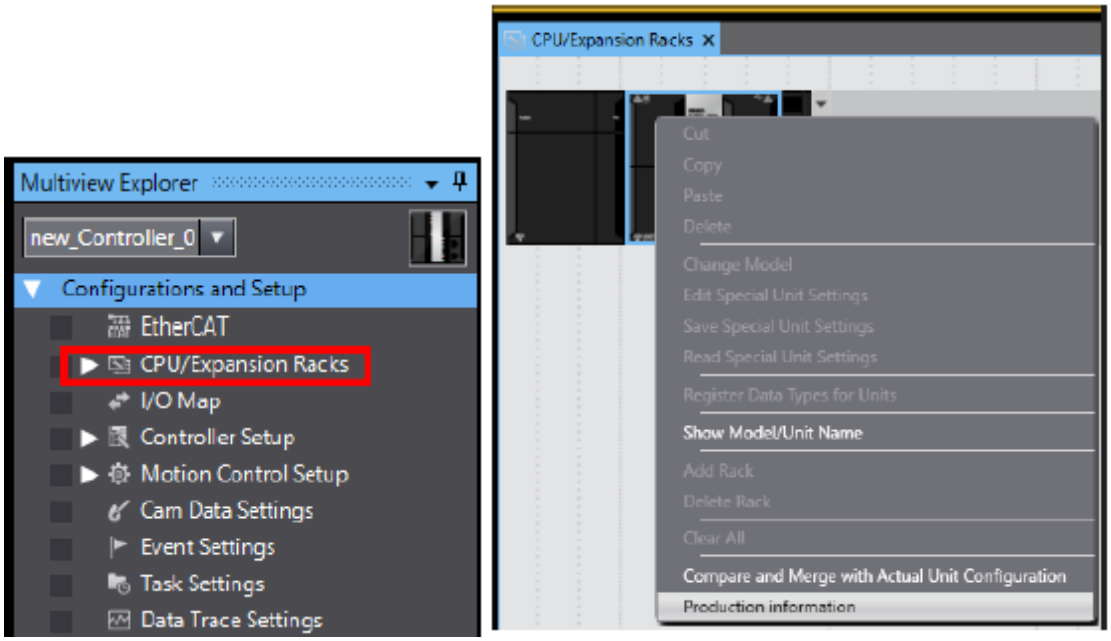
2024 年 5 月 27 日創建

附件 - 產品版本的確認方法

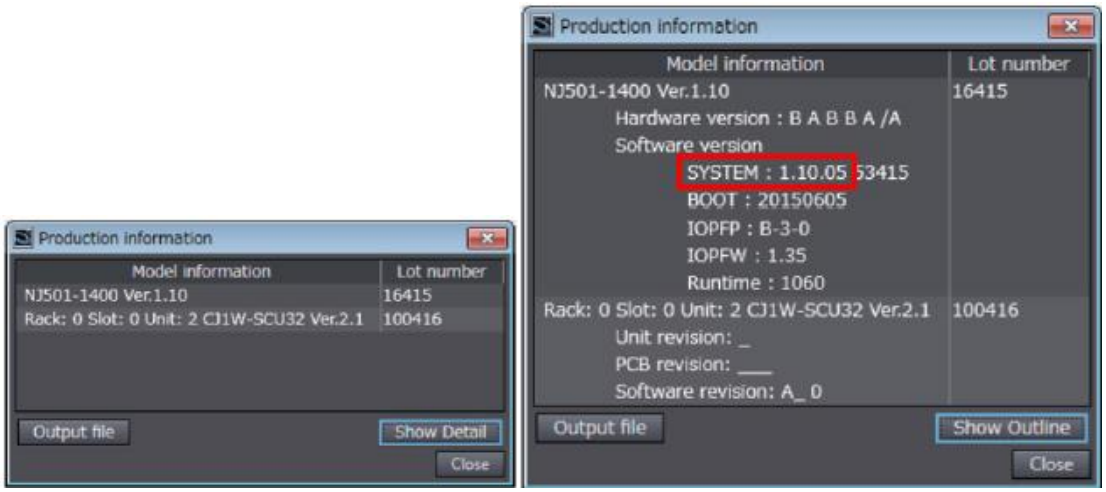
確認產品版本的方法因產品系列而異。

NJ 系列的確認方法

在 Sysmac Studio 的 Multi View Explorer 中雙擊[配置/設置] → [CPU/擴展機架]。右鍵單擊單元編輯器中的空白欄位，然後選擇[顯示產品資訊]。

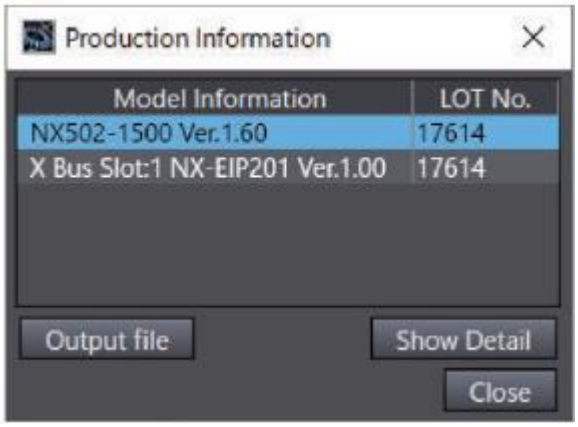


選擇[產品資訊] → [詳細顯示]。下圖顯示 Ver.1.10.05。



NX 系列的確認方法

在 Sysmac Studio 的 Multi View Explorer 中右鍵單擊[配置/設置]中的[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。