

# NJ/NX 系列機械自動化控制器通訊功能中的認證繞過漏洞

發布日期：2022 年 7 月 1 日

更新日期：2022 年 10 月 11 日

台灣歐姆龍股份有限公司

## ■ 概述

NJ/NX 系列機械自動化控制器、自動化軟體 Sysmac Studio 和 NA 系列人機介面之間的通訊功能存在使用 Hard-coded Credentials (CWE-798) 和 Authentication Bypass by Capture-replay (CWE-294) 的漏洞，攻擊者可能利用這些漏洞繞過通信連接過程中的身份驗證，然後非法存取控制器產品。

受這些漏洞影響的產品、版本的相關緩解措施和保護方法詳見下文，通過實施這些建議措施和方法，可以將這些漏洞的惡意存取風險降至最低。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。

產品系列	型號	版本
NX7 系列機械自動化控制器	所有型號	1.28 或更低
NX1 系列機械自動化控制器	所有型號	1.48 或更低
NJ 系列機械自動化控制器	所有型號	1.48 或更低
自動化軟體 Sysmac Studio	所有型號	1.49 或更低
NA 系列 人機介面	NA5-15W NA5-12W NA5-9W NA5-7W	運行版本 1.15 或更低

請參閱下列手冊，了解如何查看目標產品的版本。

- NX-series CPU Unit Hardware User' s Manual (W535)
- NX-series NX102 CPU Unit Hardware User' s Manual (W593)
- NX-series NX1P2 CPU Unit Hardware User' s Manual (W578)
- NJ-series CPU Unit Hardware User' s Manual (W500)

請參閱上述手冊中的「Checking Versions」部分

- NA-series Programmable Terminal Hardware User' s Manual (V117)
- NA-series Programmable Terminal Hardware(-V1) User' s Manual (V125)  
請參閱上述手冊中的「System Menu Overview」部分（運行版本位於系統界面的左下方區域）
- Sysmac Studio Version 1 Operation Manual (W504)  
請參閱上述手冊中的「Displaying and Registering Licenses」部分

## ■ 說明

由於 NJ/NX 系列機械自動化控制器、自動化軟體 Sysmac Studio 和 NA 系列人機介面之間的通訊功能存在使用 Hard-coded Credentials (CWE-798) 和 Authentication Bypass by Capture-replay (CWE-294) 的漏洞，產品可能在未經授權的情況下登錄並操作。

## ■ 潛在的威脅與影響

駭客可能利用此漏洞繞過通訊過程中的認證，擅自登錄和操作控制器產品。

## ■ CVSS 評分

### 1) 使用 Hard Code 憑證 (CWE-798)

CVE-2022-34151

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H 基礎評分 9.4

### 2) 透過捕獲-回放繞過身份驗證 (CWE-294)

CVE-2022-33208

CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H 基礎評分 7.5

## ■ 緩解措施和保護方法

為了將這些惡意利用風險降至最低，歐姆龍建議客戶採取下列緩解措施。

### 1. 防毒保護

保護所有可連線控制系統的个人電腦，防止其被惡意軟體攻擊，確保安裝並維護最新版本的企業級防毒軟體。

### 2. 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。
- 使用防火牆（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。

- 使用高強度密碼並增加修改頻率。
- 安裝實物控制，確保僅授權人員可連結控制系統和設備。
- 在連接系統和設備之前，掃描病毒可以確保 USB 或類似裝置的安全性。
- 強化對遠端連接控制系統和設備的多重要素驗證。

### 3. 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，以控制系統和設備輸入/輸出數據被修改。

### 4. 資料復原

定期進行數據備份和維護，以防數據丟失。

## ■ 對策

可以透過將每個產品更新到對策版本來對應這些問題，每個產品的對策版本和各自的發布日期如下表所示，對於發布日期顯示「即將發布」的產品，我們將在確定日期後第一時間公告。

產品系列	型號	版本	發布日期
NX7 系列機械自動化控制器	所有型號	1.29 或更高	2022 年 10 月 11 日
NX1 系列機械自動化控制器	所有型號	1.50 或更高	2022 年 10 月 11 日
NJ 系列機械自動化控制器	NJ501-1300 NJ501-1400 NJ501-1500	1.49 或更高	2022 年 7 月 1 日
	上述型號以外	1.50 或更高	2022 年 10 月 11 日
自動化軟體 Sysmac Studio	所有型號	1.50 或更高	2022 年 7 月 1 日
NA 系列 人機介面	NA5-15W	運行版本	2022 年 7 月 1 日
	NA5-12W	1.16 或更高	
	NA5-9W		
	NA5-7W		

有關如何獲得及更新產品對策版本軟體的資訊，請聯繫歐姆龍營業據點或經銷商。您可以歐姆龍自動化軟體 AutoUpdate 工具，將 Sysmac Studio 更新至最新版本。

建議使用控制器的以下安全功能採取對策。有關該功能及其設置方法的詳細信息，請參閱 NJ/NX 系列 CPU 單元用戶手冊軟件（SBCA-467）“8-5 安全功能”。

- 使用安全通信功能對 Sysmac Studio 或 NA 系列與控制器之間的通信數據進行加密。

您可以防止第三方竊聽或偽造數據。

- 使用數據包過濾功能在內置 EtherNet/IP 端口的接收過程中過濾 IP 數據包。通過這樣做，可以限制來自外部的未經授權的訪問。

- 當工具在線時，使用用戶認證功能對個人用戶進行認證，以及通過僅啟用操作可以防止未經授權的訪問。

## ■ 聯絡資訊

請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)

## ■ 其他

本文檔中提到的漏洞問題和對策與美國網絡安全和基礎設施安全局（CISA）在下方報告中提到的內容相符。

適用於 ICS/SCADA 設備的 APT 網絡工具

<https://www.cisa.gov/uscert/ncas/alerts/aa22-103a>

## ■ 更新紀錄

-2022 年 7 月 1 日 最新版本

-2022 年 10 月 11 日：更新以下 2 項內容

(1) 更新【對策】中對策版本的發布日期

(2) 變更如下 CVSS 訊息

- CVE-2022-34151 CVSS

(變更前) CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:H/A:H 基礎評分 7.7

(變更後) CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H 基礎評分 9.4

- CVE-2022-33208 CVSS

(變更前) CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:L/I:H/A:H 基礎評分 6.2

(變更後) CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H 基礎評分 7.5