NJ/NX 系列機械自動化控制器中的惡意程式執行漏洞

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

在 NJ/NX 系列機器自動化控制器中，存在利用 Active Debug Code (CWE-489) 執行惡意程式的可能性。攻擊者可能利用這個漏洞非法連結控制器，並導致產品停止服務或執行惡意程式。

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

受影響的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

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。

■ 說明

在 NJ/NX 系列機器自動化控制器中，存在利用 Active Debug Code (CWE-489) 執行惡意程式的可能性。攻擊者可能利用這個漏洞非法連結控制器，並導致產品停止服務或執行惡意程式。

■ 潛在的威脅和影響

攻擊者可能利用這個漏洞引發產品鼓脹或執行惡意程式。

■ CVSS 評分

CVE-2022-33971

CVSS:3.1/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H 基礎評分 8.3

■ 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個人電腦，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。
- 使用防火墻（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，以防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

可將每個產品版本更新到對策版本來對應漏洞。 每個產品的對策版本和各自的發布日期如下表示。

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

有關如何獲得及更新產品對策版本韌體的資訊，請聯繫歐姆龍營業據點或經銷商。您可以安裝 Omron Automation Software Auto Update(歐姆龍自動化軟體自動更新)工具，將 Sysmac Studio 更新至最新版本。

■ 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

■ 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 最新版本：更新以下 2 項內容

（1）更新【對策】中對策版本的發布日期

（2）變更本漏洞（CVE-2022-33971）的 CWE 編號及 CVSS 評分

（變更前）Authentication Bypass by Capture-replay（CWE-294）

CVSS:3.1/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H 基礎評分 7.6

（變更后）Active Debug Code（CWE-489）

CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H 基礎評分 8.3