機械自動化控制器 NJ/NX 存在數據真實性驗證不足的漏洞

發佈日期：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 系列存在數據真實性驗證不足（CWE-345）的漏洞。攻擊者可利用本漏洞使控制器產品無法檢測到產品內的使用者程式已被篡改。

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。

■對象產品

受此漏洞影響的產品型號及版本如下所示。

- 機械自動化控制器 NJ 系列 CPU 單元所有版本
- 機械自動化控制器 NX 系列 CPU 單元所有版本

■漏洞內容

機械自動化控制器 NJ/NX 系列存在數據真實性驗證不足（CWE-345）的漏洞，攻擊者可利用本漏洞使控制器產品無法檢測到產品內的使用者程式已被篡改。

■CVSS 評分

數據真實性驗證不足（CWE-345）

CVE-2024-33687

CVSS：3.1/AV：N/AC：H/PR：N/UI：N/S：U/C：L/I：L/A：N 基礎評分 4.8

■對策方法

將各產品更新至對策版本以應對漏洞。

1. 使用沒有使用者程式恢復資訊的傳輸功能 通常，將用戶程式從 Sysmac Studio 傳輸到 CPU 單元時，用於恢復程式的資訊也會被傳輸。此時，由於本功能不傳輸用於恢復程式的資訊，因此使用者程式無法被篡改。確認使用方法，請參見以下手冊的“沒有使用者程序恢復資訊的傳輸功能”。

・NJ/NX 系列 CPU 單元 使用者手冊 軟體篇（SBCA-CN5-467）

■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. 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。

2. 防止未經授權的存取，

   推薦採取以下措施：

   - 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. 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

■謝辭

Microsoft 公司 CPS Research Team 的 Tamir Ariel 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。

■更新記錄

2024 年 5 月 27 日創建