變頻器/伺服用支援軟體CX-Drive中

基於堆疊的緩衝區溢出漏洞

發佈日期：2023年4月24日
更新日期：2023年8月1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，我們發現在變頻器/伺服用支持軟體CX-Drive中存在基於堆疊的緩衝區溢出漏洞（CWE- 122）。 本地攻擊者可惡意利用該漏洞引發信息洩露，或在受影響的CX-Drive的安裝上執行任意代碼。惡意利用該漏洞需要使用者的操作，使用者打開惡意SDD檔是攻擊者進行攻擊的必要條件。

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。

■受影響產品

受本漏洞影響的產品型號及版本如下所示。

系列	型號	適用版本
CX-Drive	全型號	所有版本

請參考以下手冊以確認適用產品的版本：

・CX-Drive 操作使用者手冊（SBCE-375）

■CVSS 評分

基於堆疊的緩衝區溢出漏洞（CWE-122）

CVE-2023-27385

CVSS：3.1/AV：L/AC：L/PR：N/UI：R/S：U/C：H/I：H/A：H 基礎評分 7.8

■減輕措施/解決方法

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。

5. 採用新型軟體工具和控制器

   - 自動化軟體 Sysmac Studio
   - 控制器 NJ/NX/NY 系列

■謝辭

Michael Heinzl先生通過JPCERT/CC報告了本漏洞。
我們在此感謝發現並報告此漏洞的Michael Heinzl先生。

■更新記錄

2023/4/24 建立
2023/8/1 更新適用版本