CX-Programmer 存在越界讀取漏洞

發佈日期：2024 年 4 月 22 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 CX-Programmer 存在越界讀取（CWE-125）漏洞。攻擊者可利用本漏洞讀取敏感信息，導致系統崩潰。

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。

此外，為了確保您安心使用本產品，我們還為受該漏洞影響的產品準備了安全增強的對策版本。您可在下文“對策方法”處查找對應的對策版本。

■對象產品

受本漏洞影響的產品型號及版本如下所示。

產品名稱	型號	適用版本
CX-Programmer	CX-One CXONE-AL□□D-V4 附帶	Ver.9.81 以下

確認對象產品版本的方法，請參見以下手冊的“功能一覽”中記載的“版本資訊”。

- CX-Programmer Ver.9.□操作手冊（SBCA-CN5-337）

■漏洞內容

CX-Programmer 存在越界讀取（CWE-125）漏洞。攻擊者可利用這些漏洞讀取敏感資訊，導致系統崩潰。

■CVSS 評分

越界讀取（CWE-125）

CVE-2024-31412

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

■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佈日期見下表。

產品名稱	型號	對策版本	對策版本推出時間
CX 程式師	CX-One CXONE-AL□□D-V4 附帶	Ver.9.82 以上	2024 年 4 月 22 日

上述對策版本的獲取途徑及更新方法，請諮詢本公司銷售視窗。

■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

■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

2024 年 4 月 22 日創建