CX-Programmer 中的越界讀取漏洞

發布日期：2025 年 2 月 17 日

最新更新日期：2025 年 3 月 10 日

台灣歐姆龍股份有限公司

■ 概述

CX-Programmer 中存在越界讀取漏洞 (CWE-125)，攻擊者可能利用此漏洞讀取敏感資訊或導致應用程式崩潰。

受此漏洞影響的產品和版本以及緩解措施和防護措施如下所示，請務必實施這些建議的緩解措施和防護措施，以最大限度地降低這些漏洞被利用的風險。此外，為了確保客戶安心使用我們的產品，我們為每款產品準備了安全強化的應對措施版本，請採取本文對策部分所述的對策。

■ 受影響產品

受影響產品及其版本如下所示。

FA 整合軟體 CX-One

產品系列	型號	版本
CX-Programmer	CX-One Ver. 4 (CXONE-AL[][]D-V4) * CX-Programmer 包含在 CX-One 軟體內	Ver. 9.83 以下

請參閱下列手冊中的「Technical Specifications」內的「About CX-Programmer」，了解如何查看目標產品的版本。

- CX-Programmer Ver.9.[] Operation Manual (W446)

■ 說明

CX-Programmer 存在名為「越界讀取」(CWE-125)的漏洞，攻擊者可利用該漏洞讀取 CX-Programmer 中的敏感訊息，或導致 CX-Programmer 崩潰。

不過，安裝 CX-Programmer 的電腦以及連接 CX-Programmer 的 PLC 不會受到影響。

■ CWE, CVE, CVSS 評分

越界讀取 (CWE-125)

CVE-2025-0591

CVSS: 3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H 基本值 7.8

■ 對策

請將您的 CX-Programmer 更新至應對措施版本以修復此漏洞，各產品的應對措施版本及發布日期如下表所示。

FA 整合軟體 CX-One

產品系列	型號	版本	對策發布時間
CX-Programmer	CX-One Ver. 4 (CXONE-AL[] []D-V4) * CX-Programmer 包含在 CX-One 軟體內	Ver. 9.84 以上	2025 年 1 月 8 日

有關如何取得更新產品對策版本的信息，請諮詢本公司營業窗口。

或您可以使用已安裝的 OMRON 自動化軟體自動更新工具將 CX-One 更新至最新版本。

■ 緩解措施和保護方法

為了將這些風險降至最低，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身分驗證。

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。

■ 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

■ 致謝

Michael Heinzl 透過 JPCERT/CC 回報了此漏洞。

感謝 Michael Heinzl 發現並回報此漏洞。

■ 更新紀錄

- 2025 年 2 月 17 日 發布

- 2025 年 3 月 10 日 更新說明文字