自動化軟體 Sysmac Studio 中不正確授權（CWE-863）漏洞

發布日期: 2024 年 11 月 1 日
台灣歐姆龍股份有限公司

■ 概述

自動化軟體 Sysmac Studio 軟體中存在不正確授權 (CWE-863) 漏洞，攻擊者可以利用此漏洞對受資料保護功能保護的程式進行未經授權的存取。以下列出了受此漏洞影響的產品、版本和緩解/解決方法。透過實施我們推薦的緩解措施和變通方法，您可以最大限度地降低利用此漏洞的風險。另外，為了讓客戶更安心地使用產品，我們現在準備了產品安全性增強的版本。關於針對每個產品所提供的對策版本，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。

Sysmac Studio 軟體

產品系列	型號
SYSMAC-SE2[][][]	所有型號

請參閱下列手冊，了解如何查看目標產品的版本。

- Sysmac Studio Version 1 Operation Manual (W504)

■ 說明

由於 Sysmac Studio 軟體中存在不正確授權（CWE-863）漏洞，受資料保護功能保護的程式可能會被非法存取。

■ 潛在的威脅與影響

駭客可能利用此漏洞繞過通訊過程中的認證，擅自登錄和操作控制器產品。

■ CVSS 評分

不正確授權（CWE-863）

CVE-2024-49501

CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N 基本值 5.7

■ 對策

可以透過使用無原始碼程式庫來對抗該漏洞，其保護能力比資料保護更強。我們建議您按照以下步驟使用無原始碼程式庫。

1. 將產品更新至正確版本

Sysmac Studio 軟體

產品系列	對策版本	對策提供時間
SYSMAC-SE2[][][]	Ver.1.60 以上	2024 年 10 月 16 日

有關如何取得和更新對策版本的信息，請參閱以下連結。

https://www.fa.omron.co.jp/product/tool/install_manual/index.html

2. 將您想要保護的程式儲存到無原始碼庫中

關於如何使用無原始碼庫，請參閱 Sysmac Studio Version 1 Operation Manual (W504)。

■ 缓解措施和保護方法

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。
- 使用防火墙（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。
- 使用高強度密码並增加修改頻率。
- 安裝實物控制，确保僅授權人员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。

■更新紀錄

-2024 年 11 月 1 日 最新版本