可程式控制器 CS/CJ 系列 EtherNet/IP 單元存在多個因 OpenSSL 引起的漏洞

發佈日期：2024年11月1日

台灣歐姆龍股份有限公司

■概要

在可程式控制器 CS/CJ 系列 EtherNet/IP 單元中使用的 OpenSSL 函式庫被發現存在觀測可能的不一致（CWE-203）、雙重釋放（CWE-415）、已釋放記憶體使用（CWE-416）等漏洞。攻擊者可能利用這些漏洞導致該控制器產品的資訊洩漏或服務中斷（DoS）。

以下列出受此漏洞影響的產品、版本以及減輕風險的對策與迴避方法。透過執行我們建議的對策與迴避方法，可以將此漏洞被利用的風險降至最低。此外，為了讓客戶更加安心地使用產品，我們已準備了針對本次安全性強化的對策版本。關於各產品的對應版本，請參考本文中的對策方法，並請配合實施相關對策。

■受影響產品

受本漏洞影響的產品型號及版本如下所示。

型號	受影響的版本	批號（製造日期）
CS1W-EIP21S	版本 1.02 及以前的版本	241014以前（2024/10/14以前）
CJ1W-EIP21S	版本 1.02 及以前的版本	241014以前（2024/10/14以前）

確認「受影響版本」和「批號」的方法，請參考《CS/CJ 系列 EtherNet/IP 使用者手冊（SBCD-342）》中的「批號及單元版本」部分。

■漏洞內容

攻擊者可能利用可程式控制器 CS/CJ 系列 EtherNet/IP 單元中使用的 OpenSSL 函式庫的多個漏洞，導致該控制器產品的資訊洩漏或服務中斷（DoS）的風險。

■CVSS 評分

(1) 可觀察的不一致（CWE-203）

CVE-2022-4304

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N 基礎評分 5.9

（2）二重解放（CWE-415）
CVE-2022-4450
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H 基礎評分7.5

（3）使用已釋放的記憶體（CWE-416）
CVE-2023-0215
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H 基礎評分7.5

■對策方法
可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。

型號	對策版本	批號	對策版本 推出時間
CS1W-EIP21S	版本 1.03 及以後的版本	241015 及以後的批號	2024年10月15日
CJ1W-EIP21S	版本 1.03 及以後的版本	241015 及以後的批號	2024年10月15日

上述對策版本的獲取途徑及更新方法，請諮詢本公司銷售窗口。

■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。

■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

■更新記錄

2024年11月1日 建立