SOLAR-OT 部署的 CHIYU 感測器發生事故后的補救行動

部署最新版本的韌體，並加固 SOLAR-OT 的監控平臺

作者	審批人
Deirdre STARSKY，技術項目經理	Elena PIZARI，工業總監

目的

本文檔詳細說明了 SOLAR-OT 部署的訪問控制系統在發生事故后的 2 項補救措施：

1. 對所有系統緊急部署韌體更新
2. 加強監控平臺的配置

1. 緊急部署韌體更新

Chiyu 製造商為「SEMA」門禁控制系統開發了韌體更新，糾正了漏洞 => 必須由 SOLAR-OT 緊急部署在所有站點上

這是要在 SEMAC S2 上部署的韌體版本號（佔園區的 67%）：670VYJLN
這是要在 SEMAC S3V3 上部署的韌體版本號（佔園區的 33%）：628AUYSD

2. 加強監控平臺的配置

配置

其目的是通過只安裝必要的服務和設備，限制可用於實施攻擊的技術要素。

為提高安全級別，需要進行加固，包括：

- 限制平臺的功能
- 控制平臺的硬體元素

A. 更改預設配置

每個組件都根據標準進行配置，包括：

- 技術帳戶和相關的身份驗證元素
- 使用的網路連接埠
- 安裝和工作目錄
- 對目錄和文檔的訪問權限
- 用於運行服務或進程的帳戶以及與該帳戶關聯的權限
- 安全元素的配置文檔，特別是可追溯性。

B. 對可訪問功能的限制

僅保留對平臺的操作和安全至關重要的模塊，並對其進行適當的配置、定期維護和監控。

因此，操作員會分析平臺的技術功能，排除已安裝但未使用的服務或功能。

每個硬體或軟體配置都作為參考配置進行盤點。

C. 連接元素的盤點清單

操作員對構成平臺和製圖的元素進行完整的技術盤點。
盤點清單包括可永久或臨時，物理或遠程連接到平臺的設備（工作站，伺服器，設備等）。

如果第三方連接到平臺，操作員將其記錄在製圖中，並在風險分析中將其考慮在內。

D. 使用受控元素

操作員直接管理元素，包括：

- 部署更新
- 管理要素
- 遠程配置

分區

平臺遵循分段邏輯，將每個子系統限制為自身操作，以便：

- 限制攻擊的範圍
- 遏制可能的攻擊
- 限制漏洞的影響
- 允許調整每個子系統的安全級別

分區同時適用於物理和邏輯方式。

A. 子系統分段

子系統分段根據以下標準進行：

- 功能
- 數據保護級別
- 暴露水平
- 安全級別

子系統之間的任何連接都應以功能需求為依據。

B. 物理分區

伺服器專用於最關鍵的應用程式

C. 邏輯分區

存儲在伺服器上的任何數據都會事先加密。 每個子系統都遵循自己的加密機制。

子系統之間的所有通信都通過加密和經過身份驗證的虛擬專用網路。

遠程訪問

A. 公共訪問

公共訪問遵循 HTTPS 協議，平臺通過提供伺服器證書進行身份驗證。

對平臺用戶實施雙因素身份驗證。

B. 遊牧訪問

遊牧工作站的配置是為了建立經過身份驗證和加密的通道，以到達平臺。
無法停用通道，無法訪問互聯網或局域網。
系統分區和數據分區已完全加密

工作站設置了雙因素身份驗證。

網路過濾

除了分區之外，還建立了過濾機制。

A. 過濾點

子系統互連是應用周邊和本地過濾的主要過濾點。

B. 過濾規則

全域流矩陣包括當前的過濾規則。 它每年更新。

C. 實施

過濾由基於授權列表原則的專用防火牆提供。