中華人民共和國香港特別行政區政府
數字政策辦公室

HKCERT 香港網絡安全事故協調中心

政府資助計劃 Government-funded programme

物聯網

數碼顯示屏保安研究報告

免責聲明

香港生產力促進局屬下的香港網絡安全事故協調中心（HKCERT）保留不時修改文件的權利而無須另行通知。

HKCERT 已盡力確保本文件所含資料均來自可靠來源，對任何錯誤或遺漏或使用相關資料所招致的結果概不負責。本文件上的所有資料均以當時情況提供，不擔保其完整性、準確性、及時性、或使用相關資料所招致的結果，亦不作任何明示或隱含的保證，包括但不限於其性能保證、適售性和特定用途的適用性。

本文件包含的資料僅供參考。信賴或使用相關資料由讀者自行承擔風險。本文件的任何內容均不得在任何程度上替代讀者的獨立調查和合理的技術和商業判斷。在任何情況下，香港網絡安全事故協調中心、香港生產力促進局、或其合作夥伴、員工或代理商，均不對你或任何人信賴本文件相關資料做出的任何決定或行動，或任何後果性，特殊或類似的損害承擔責任。

版權

目錄

1. 簡介

數碼顯示屏在各行各業中很受歡迎，用於推廣產品和向客戶展示資訊。作為物聯網裝置，它可能成為黑客進行網絡攻擊的目標。因此，HKCERT 對 8 個數碼顯示屏進行了保安研究。其研究和觀察結果與保安建議一起提供予公眾和數碼顯示屏用戶參考。

此保安研究旨在確定與普遍數碼顯示屏系統相關的潛在漏洞，並於 2024 年 10 月進行。本報告亦記錄了研究結果和保安建議等詳細資訊。

此保安研究的目標是：

- 對選定的數碼顯示屏及其用戶端應用程式和網頁管理平台應用程式進行保安測試
- 識別選定的數碼顯示屏和網頁管理平台中的保安風險
- 建議保安措施以應對已識別的風險

2. 保安測試方法和研究結果概要

2.1. 保安測試方法

數碼顯示屏系統通常設置在無線網路中，顯示屏裝置通常運行 Android 或 Windows 作業系統。用戶可以透過登入顯示屏或內容管理系統 (CMS) 來上傳媒體、調整螢幕設定和設定時間表等來更新顯示內容。當內容在管理系統中完成儲存後，其將會發送至顯示屏裝置進行顯示。以下圖示說明從用戶發送更新內容至顯示屏裝置的過程。

圖 1 - 從用戶電腦發送更新內容至顯示屏裝置

本研究包含四個不同品牌的 Windows 和 Android 作業系統數碼顯示屏的測試結果，分別是 8 台裝置和其相應的網頁管理平台。以下列表為進行了保安測試所選定的數碼顯示屏：

品牌	作業系統	數碼顯示屏 測試編號	顯示屏網頁管理 平台 *	顯示屏網頁管理平台 測試編號
A	Windows	**A1**	N/A	N/A
	Android	**A2**		
B	Windows	**B1**	有	**B1P**
	Android	**B2**	有	**B2P**
C	Windows	**C1**	有	**CP**

	Android	**C2**		
D	Windows	**D1**	有	**DP**
	Android	**D2**		

列表 2-1. 保安測試所選定的數碼顯示屏

* 品牌 A 數碼顯示屏方案不包含網頁管理平台，因此並無相關保安測試；品牌 B 分別為 Windows 和 Android 作業系統的顯示屏提供不同的網頁管理平台。

此保安測試中使用了灰盒方法，並提供了數碼顯示屏的網絡環境、IP 地址，以及用於在網頁管理平台進行身份驗證的憑證。

保安測試方法的流程如下：

2.2. 研究結果概要

本節總括了保安測試中的研究結果，並根據它們的風險等級歸納在以下列表。這些研究結果已被確定在《OWASP Top 10》[1]和《OWASP IoT Top 10》裡 [2]。

風險等級	**研究結果總數**	**顯示屏網頁管理平台上的研究結果數量**	**數碼顯示屏裝置上的研究結果數量**
高	**10**	5	5
中等	**6**	4	2
低	**4**	2	2
總數	**20**	11	9

列表 2-2. 研究結果概要

在保安測試中共有了 20 個研究結果。其中 11 個是在顯示屏網頁管理平台中存在的風險，9 個是在數碼顯示屏裝置中存在的風險。

3. 保安測試風險評級和定義

在保安測試中，研究結果的風險就其影響和可能性進行了分析。它們會被分配一個風險等級，如以下風險評級表所示：

風險		可能性		
		高	中等	低
影響	高	高	高	中等
	中等	高	中等	低
	低	中等	低	低

列表 3-1. 風險評級表

以下列表總括了風險影響和可能性等級的定義：

影響	描述
高	利用該漏洞可能會使主機受到威脅，或者數據/服務/用戶可能會受到嚴重影響。
中等	僅憑漏洞可能不會導致主機受到直接危害。但當與其他漏洞結合使用或滿足某些先決條件時，可能會直接/間接導致系統/數據/用戶的保安完全/部分受到損害。
低	服務/數據/用戶可能會受到漏洞的影響，但不是嚴重和致命傷的影響。

列表 3-2. 風險影響定義

可能性	描述
高	輕易訪問攻擊範圍或漏洞利用代碼/工具隨時可用。
中等	訪問攻擊範圍的機會有限，或者需要深入的了解、專業技能或知識才能利用。
低	對攻擊範圍的訪問受限。只能在滿足某些先決條件或理論上才利用。

列表 3-3. 風險可能性定義

4. 關於顯示屏網頁管理平台的研究結果

4.1. 研究結果概要

以下列表總括了保安測試中研究結果的風險數量。

研究結果編號	簡述	風險
IoT-WEB-01	敏感數據洩露	高
IoT-WEB-02	不安全的密碼雜湊	高
IoT-WEB-03	過時的程式碼庫	高
IoT-WEB-04	SQL 注入	高
IoT-WEB-05	訪問控制失效	高
IoT-WEB-06	繞過客戶端驗證	中等
IoT-WEB-07	跨網站指令碼	中等
IoT-WEB-08	固定通訊	中等
IoT-WEB-09	未經身份驗證可以訪問的檔案	中等
IoT-WEB-10	更改密碼不需要重新驗證	低
IoT-WEB-11	不安全的 HTTP 使用	低

列表 4-1. 研究結果列表 – 顯示屏網頁管理平台

	顯示屏網頁管理平台測試編號 *			
研究結果編號	***B1P***	***B2P***	***CP***	***DP***
IoT-WEB-01	-	-	-	受影響
IoT-WEB-02	-	受影響	-	受影響
IoT-WEB-03	受影響	受影響	受影響	受影響
IoT-WEB-04	-	-	-	受影響
IoT-WEB-05	-	-	-	受影響
IoT-WEB-06	-	-	-	受影響
IoT-WEB-07	-	受影響	-	-
IoT-WEB-08	受影響	-	受影響	-
IoT-WEB-09	受影響	-	受影響	-
IoT-WEB-10	-	受影響	-	受影響
IoT-WEB-11	受影響	受影響	受影響	受影響

列表 4-2. 漏洞列表 – 顯示屏網頁管理平台

* 「-」 代表不受影響。

4.2. 顯示屏網頁管理平台的詳細結果

4.2.1. 高風險研究結果

4.2.1.1. IoT-WEB-01： 敏感數據洩露

風險等級	高
受影響測試編號	DP
OWASP Top 10	A01：2021 - Broken Access Control A05：2021 - Security Misconfiguration

詳情

此研究結果指出並訪問控制不足，允許任何用戶訪問端點並檢索敏感資訊。公開的端點允許用戶查看敏感數據，包括用戶清單、密碼、角色和其他敏感詳細資訊。此漏洞可能會導致嚴重的保安問題，例如用戶類比、帳戶接管和更廣泛的系統入侵。

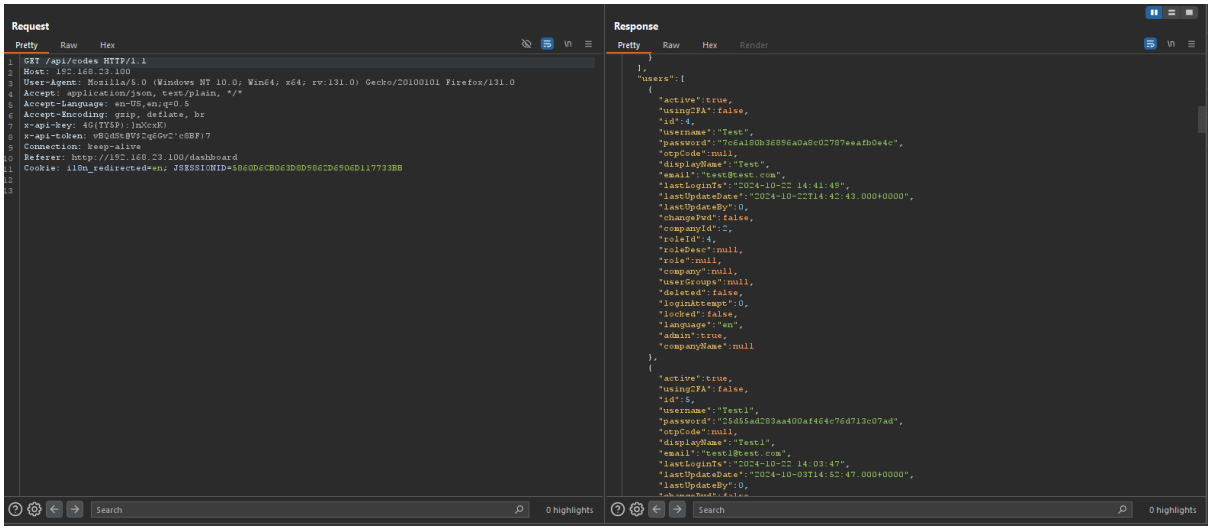

圖 2 - 列出所有用戶、其密碼雜湊和其他敏感數據

4.2.1.2. IoT-WEB-02： 不安全的密碼雜湊

風險等級	高
受影響測試編號	B2P、DP
OWASP Top 10	A02：2021 - Cryptographic Failures

詳情

管理平台使用 MD5 作為密碼雜湊演算法，按照現代標準，這不是適合密碼的雜湊演算法。此外，受影響的管理平台未使用密碼鹽（Password Salt）作為雜湊函數輸入的一部分。這使得攻擊者更容易破解雜湊值。

例如，用戶「Test」的密碼雜湊為：「25d55ad283aa400af464c76d713c07ad」。由於 MD5 雜湊中沒有使用加密鹽（Cryptographic Salt），並且其密碼較弱，攻擊者可以通過對公共雜湊資料庫進行查找來輕易恢復密碼。「Test」帳戶的密碼為「12345678」。

這指出其密碼雜湊是簡單的 MD5 雜湊，沒有適當的加密鹽（Password hash=MD5（password））。未加鹽（Unsalted）的 MD5 雜湊已被認定為較容易受到各種類型的攻擊（例如彩虹表等預計算密碼攻擊，它會生成已知密碼和相應 MD5 雜湊的清單並儲存在資料庫中以供將來查找）。擁有密碼雜湊的攻擊者可以毫不費力地從雜湊中恢復純文字密碼。

即使與適當的加密鹽一起使用，MD5 也不再被視為密碼的強雜湊演算法。例如，香港特別行政區政府的《資訊科技保安指引[G3]》要求至少應使用 SHA-2 進行用戶密碼的密碼雜湊處理，然而 MD5 被認為比 SHA-2 較弱。

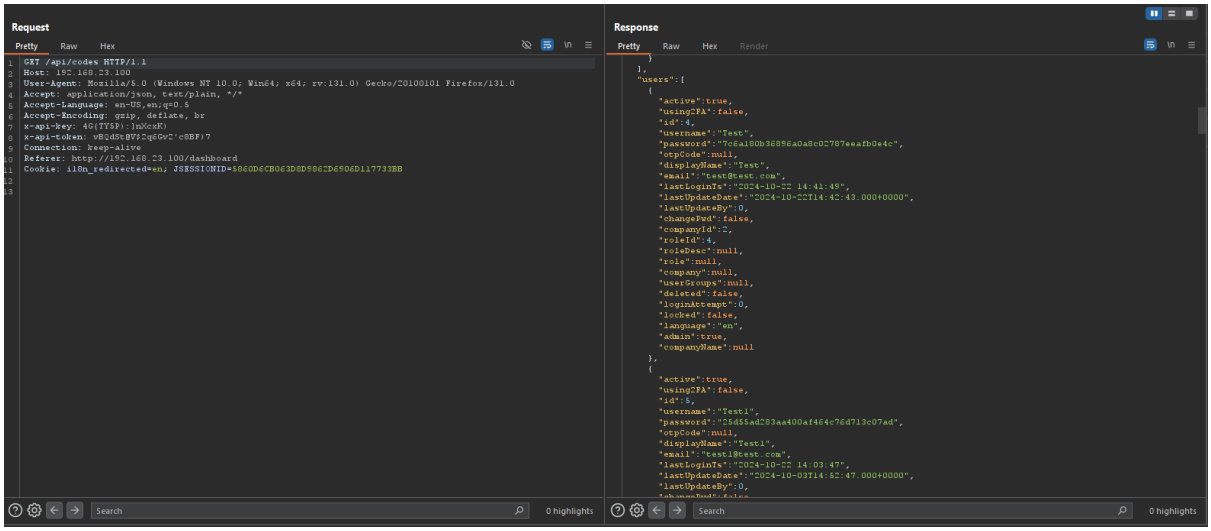

圖 3 - 檢測到未加鹽（Unsalted）的 MD5 雜湊

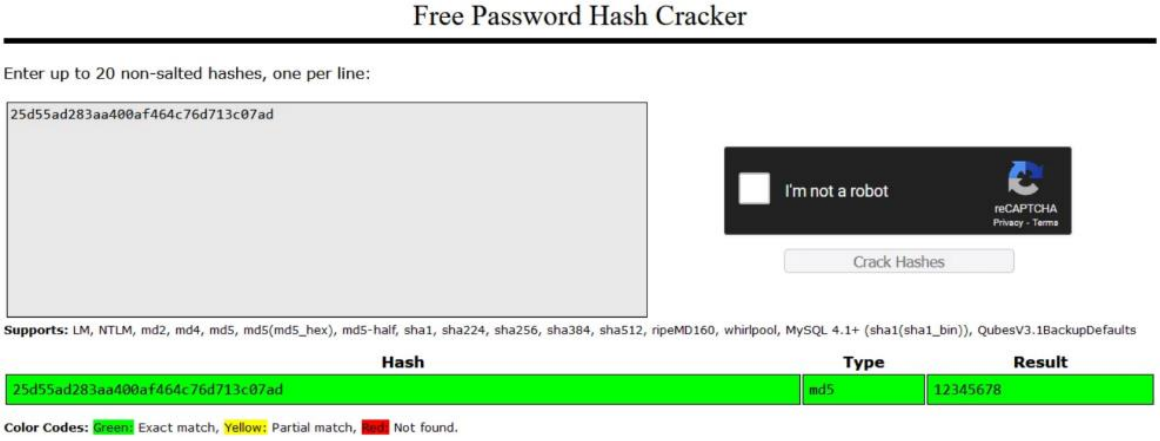

圖 4 - 25d55ad283aa400af464c76d713c07ad > 12345678

4.2.1.3. IoT-WEB-03： 過時的程式碼庫

風險等級	高
受影響測試編號	B1P、B2P、CP、DP
OWASP Top 10	A06：2021 - Vulnerable and Outdated Components

詳情

B1P、B2P、CP 和 DP 管理平台使用具有已知漏洞的過時程式碼庫。攻擊者有機會利用這些漏洞，因而帶來一些保安風險。

易受攻擊的程式碼庫如下：

受影響的管理平台編號	**版本**	**已知漏洞**	**最高風險等級（CVSS 評分）**
DP	JavaScript： bootstrap 4.4.1	CVE-2024-6531 CVE-2024-6484	中等 （5.9）
B2P	JavaScript： jQuery 1.8.3	CVE-2020-7656 CVE-2020-11022 CVE-2020-11023 CVE-2019-11358 CVE-2015-9251 CVE-2012-6708	中等 （6.5）
B1P CP	JavaScript： ExtJS 4.1.1.1	CVE-2007-2285 CVE-2018-9046	高 （7.8）

列表 4-3. 易受攻擊的程式碼庫

4.2.1.4. IoT-WEB-04： SQL 注入

風險等級	高
受影響測試編號	DP
OWASP Top 10	A03：2021 - Injection

詳情

DP 管理平台在將用戶輸入連接到 SQL 查詢之前無法正確清理用戶輸入。在輸入欄位中輸入單引號時，會觸發 SQL 錯誤，指出輸入在 SQL 查詢中直接連接，而沒有進行充分的轉義或參數化，從而導致 SQL 語法中斷。

儘管輸入導致 SQL 錯誤，但在保安測試期間，沒有允許數據提取或指令執行的完整概念驗證（PoC）漏洞利用成功。這可能是由於在資料庫交互中使用了「PreparedStatement」回調，這通常通過保安地處理一些輸入參數來降低 SQL 注入風險。但如果仍然將一些數值連接到 SQL 語句，而沒有進行適當的輸入清理和驗證，這會令管理平台容易受到攻擊。用戶控制的輸入值在 SQL 語句中被多次使用，這使得構建要執行的有效語句變得更加困難。

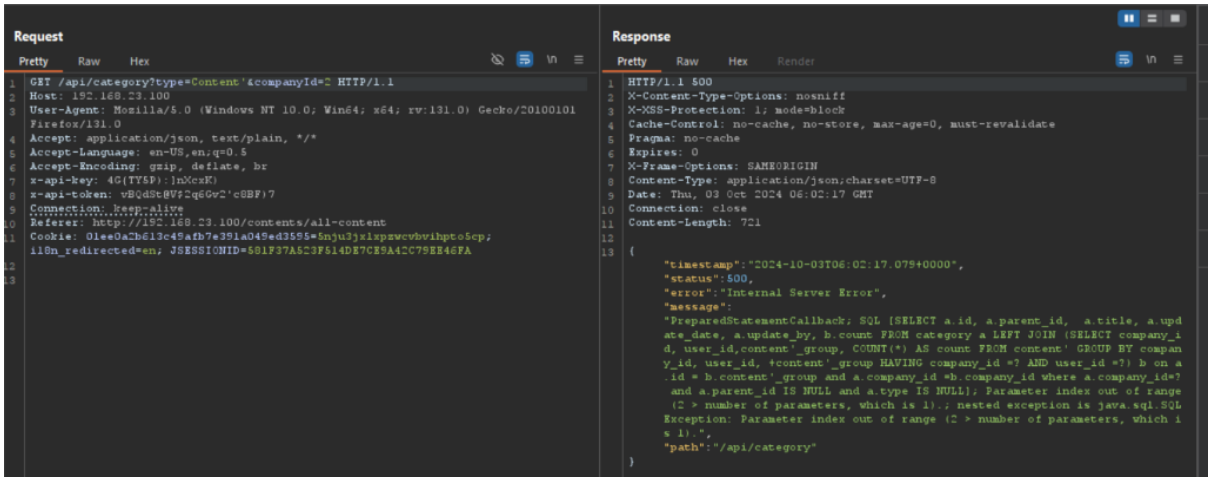

圖 5 – SQL 錯誤

4.2.1.5. IoT-WEB-05： 訪問控制失效

風險等級	高
受影響測試編號	DP
OWASP Top 10	A01：2021 - Broken Access Control

詳情

在管理平台中，不應具有特別訪問權限的常規帳戶能夠重新啟動裝置。這代表基於帳戶的訪問控制失效，從而允許權限不足的用戶執行關鍵的系統操作。這可能會導致服務終止、中斷運作並影響其他用戶。

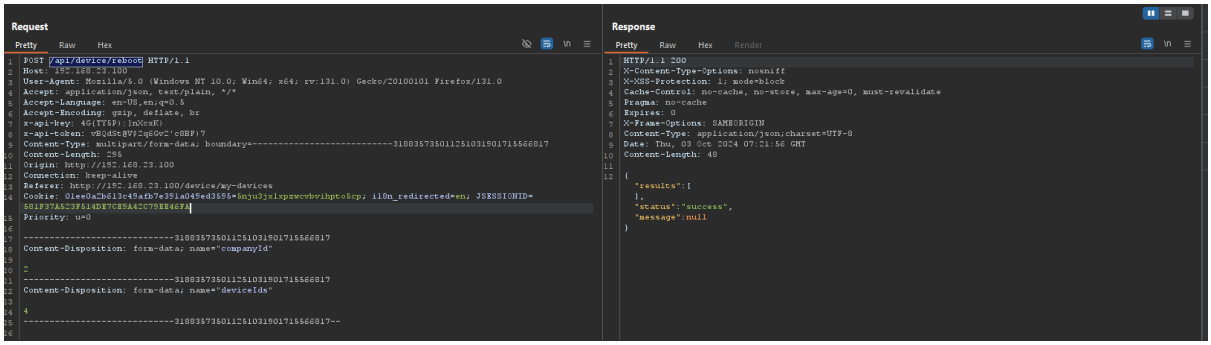

圖 6 - 用戶不應具有重新啟動的訪問權限

此外，當以普通用戶身份登錄時，左側邊欄功能表沒有「Schedule」按鈕。但是，據觀察，普通用戶可以通過直接訪問「Schedule」的 URL 連結來訪問該頁面。

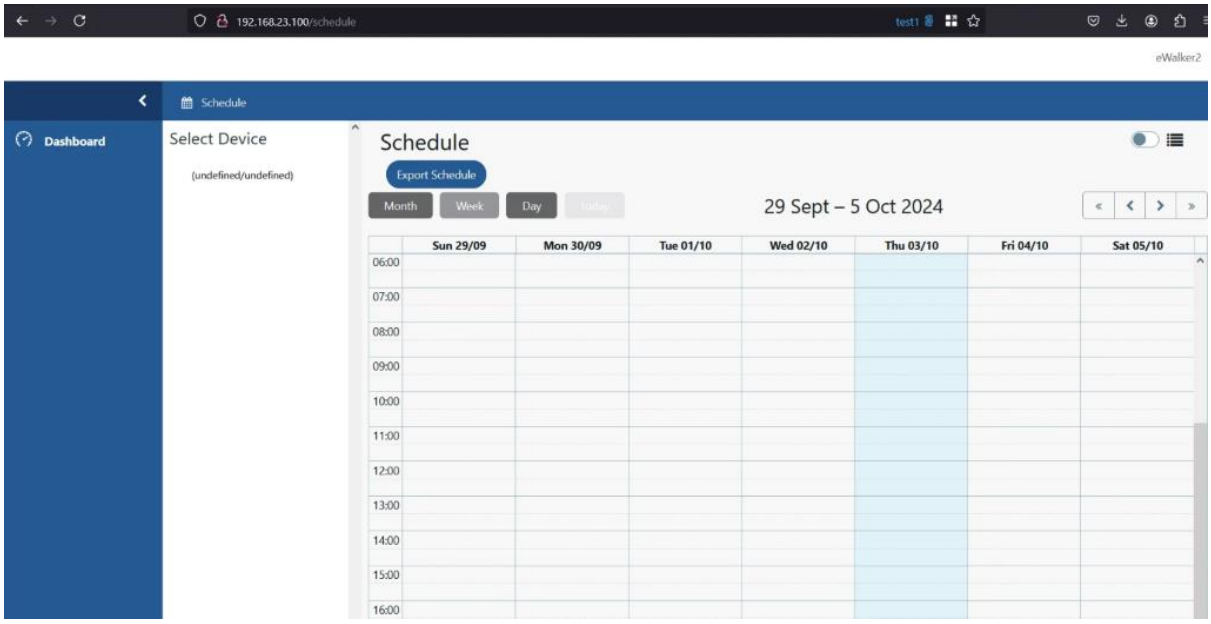

圖 7 - 左側邊欄功能表沒有「Schedule」按鈕

4.2.2. 中等風險研究結果

4.2.2.1. IoT-WEB-06： 繞過客戶端驗證

風險等級	中等
受影響測試編號	DP
OWASP Top 10	A05：2021 - Security Misconfiguration

詳情

管理平台在客戶端強制驗證 email 參數，防止用戶通過用戶界面對其進行修改。但是，email 參數被研究發現仍可修改。通過更改 HTTP 請求中的電子郵件，伺服器還是會接受更改，帳戶名稱也可以被修改。

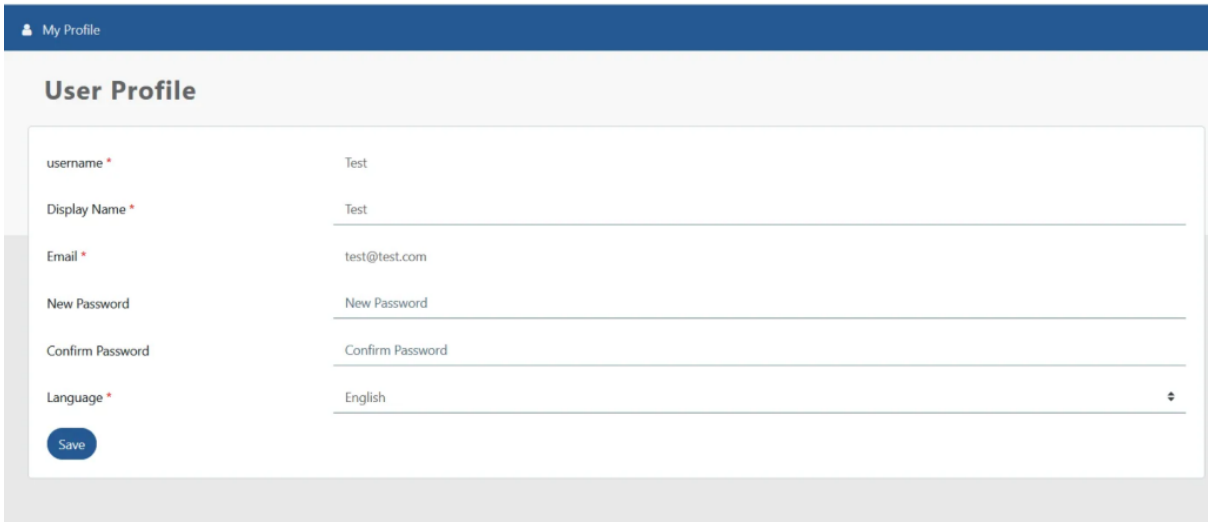

圖 8 - 無法在用戶端修改「email」參數

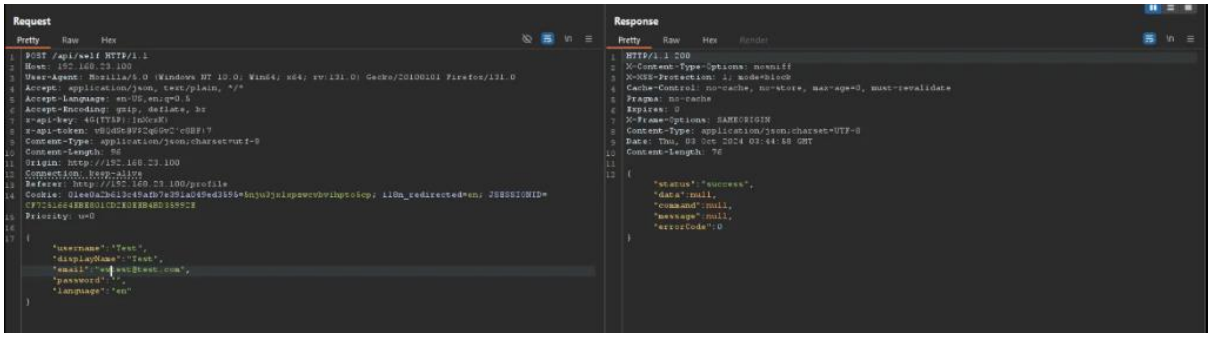

圖 9 - 成功修改伺服器端的「email」參數

4.2.2.2. IoT-WEB-07： 跨網站指令碼

風險等級	中等
受影響測試編號	B2P
OWASP Top 10	A05：2021 - Security Misconfiguration

詳情

此漏洞被研究發現可以將包含跨網站指令碼(XSS)封包的惡意文字檔上傳到管理平台。輸入「<img onerror=" alert (document.cookie) " src=a> 」在呈現到頁面上之前沒有被伺服器正確清理。因此，瀏覽器在載入顯示已上傳文件的頁面時執行指令碼，從而導致執行 alert (document.cookie)，該指令碼演示了對 Cookie 等敏感用戶數據的訪問。但是，此攻擊需要具有上傳權限的帳戶。

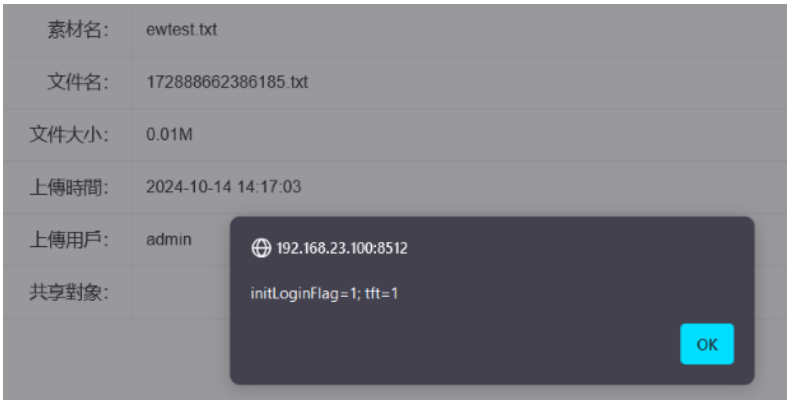

圖 10 - **成功實施 XSS Payload**

4.2.2.3. IoT-WEB-08： 固定通訊

風險等級	中等
受影響測試編號	B1P、CP
OWASP Top 10	A07：2021 - Identification and Authentication Failures

詳情

儲存通訊令牌 (Session Token) 的通訊 Cookie 在用戶登錄後保持不變。它會導致固定通訊漏洞，允許攻擊者通過在登錄前讀取或操縱其通訊令牌來冒充合法用戶。

即使在系統上成功登錄後，通訊令牌也不會更改。

圖 11 - 固定通訊攻擊流程

由於攻擊者和受害者共用相同的通訊令牌而受害者已通過身份驗證，系統使用該令牌來識別用戶的身份驗證狀態，所以攻擊者亦能夠通過身份驗證。

IoT-WEB-09：未經身份驗證可以訪問的檔案

風險等級	中等
受影響測試編號	B1P、CP
OWASP Top 10	A01：2021 - Broken Access Control

Details

在該管理平台中即使沒有身份驗證或權限，任何擁有檔案 URL 連結的人都可以訪問這些檔案。由於缺乏訪問控制，未經授權的用戶只需瀏覽到 URL 連結即可檢索檔案。

4.2.3. 低風險研究結果

4.2.3.1. IoT-WEB-10： 更改密碼不需要重新驗證

風險等級	低
受影響測試編號	B2P、DP
OWASP Top 10	A04：2021 - Insecure Design

詳情

研究發現更改密碼時不需要當前的密碼。它將允許擁有有效通訊的攻擊者在沒有憑證的情況下更改密碼。可以通過 CSRF、XSS 從事件日誌中獲得有效通訊，或者攻擊者通過瀏覽器訪問已登錄的管理平台。

4.2.3.2. IoT-WEB-11： 不安全的 HTTP 使用

風險等級	低
受影響測試編號	B1P、B2P、CP、DP
OWASP Top 10	A04：2021 - Insecure Design

詳情

B1P、B2P、CP 和 DP 管理平台通過 HTTP 而不是 HTTPS 傳輸敏感數據，例如登錄憑證或個人資訊。HTTP 不提供加密，這意味著所有數據都以純文字形式發送，很容易被網絡上的攻擊者攔截。這種缺乏加密會暴露敏感資訊，從而損害用戶隱私和管理平台數據的完整性。

5. 數碼顯示屏裝置的研究結果

5.1. 研究結果概要

以下列表總括了保安測試中研究結果的風險數量。

研究結果編號	描述	風險
IoT-DEV-01	通過紅外線進行未經授權的控制	高
IoT-DEV-02	未經授權向顯示屏發送指令	高
IoT-DEV-03	暴露的外部介面埠	高
IoT-DEV-04	啟用的觸控屏允許控制	高
IoT-DEV-05	使用 USB 裝置顯示惡意程式	高
IoT-DEV-06	未加密的數據流量	中等
IoT-DEV-07	停用 Windows 防火牆 / Windows Defender	中等
IoT-DEV-08	阻斷服務 （Denial of Service）	低
IoT-DEV-09	暴露了不必要的網絡服務	低

列表 5-1. 研究結果列表 – 數碼顯示屏裝置

	*數碼顯示屏裝置測試編號 **							
研究結果編號	***A1***	***A2***	***B1***	***B2***	***C1***	***C2***	***D1***	***D2***
IoT-DEV-01a	受影響	受影響	-	受影響	-	受影響	-	受影響
IoT-DEV-01b	-	受影響	-	受影響	-	-	-	受影響
IoT-DEV-02	-		受影響	-	受影響	受影響	-	-
IoT-DEV-03	受影響	受影響	受影響	受影響	受影響	受影響	受影響	受影響
IoT-DEV-04	受影響	受影響	受影響	影響	受影響	受影響	受影響	受影響
IoT-DEV-05	-	-	受影響	-	受影響	-	-	-
IoT-DEV-06	受影響	受影響	影響	影響	影響	受影響	受影響	受影響
IoT-DEV-07	受影響	-	-	-	-	-	受影響	-
IoT-DEV-08	受影響	受影響	受影響	受影響	受影響	受影響	受影響	受影響
IoT-DEV-09	受影響	-	受影響	-	受影響	-	受影響	-

列表 5-2. 漏洞列表 – 數碼顯示屏裝置

* 「-」 代表不受影響。

5.2. 數碼顯示屏裝置的詳細結果

5.2.1. 高風險研究結果

5.2.1.1. IoT-DEV-01： 通過紅外線進行未經授權的控制

風險等級	高
受影響測試編號	(a) 使用滲透測試工具 - A1、B1、B2、C1、C2、D1、D2 (b) 使用萬能遙控器 - A2、B2、C2、D2
OWASP IoT Top 10	I10：2018 - Lack of Physical Hardening

詳情

在受影響的顯示屏中研究發現存在紅外線 (IR) 感測器。攻擊者可以使用紅外線遙控器控制顯示屏，啟用如返回主功能表、打開瀏覽器訪問其他網站甚至關閉顯示屏等操作。

（a） 使用滲透測試工具

在指令暴力破解期間，可以找出紅外線信號地址和指令的清單。這些可用於使用滲透測試工具的內置紅外線模組或 NEC 紅外線發送器來控制顯示屏的監視器/系統。

（b） 使用萬能遙控器

萬能遙控器也可能能夠執行一些指令。萬能遙控器通常帶有各種電視品牌和型號的指令資料庫。攻擊者可以通過使用通用遙控器上的搜索功能找到正確的代碼集來控制顯示屏。

圖 12 - 萬能遙控器包括搜索正確指令的功能

使用萬能遙控器，我們可以控制 A2、B2 和 C2 顯示屏內置的系統。我們還可以使用遙控器的搜索功能關閉 D2 的系統。在某些情況下，關閉顯示螢幕無法反映在管理平台中。因此，不進行物理檢查便無法檢測到某些攻擊。

5.2.1.2. IoT-DEV-02： 未經授權向顯示屏發送指令

風險等級	高
受影響測試編號	*B1*、*C1*、*C2*
OWASP IoT Top 10	I02：2018 - Insecure Network Services I03：2018 - Insecure Ecosystem Interfaces I07：2018 - Insecure Data Transfer and Storage

詳情

據觀察，如果攻擊者能夠向顯示屏發送數據包，則攻擊者可以冒充伺服器向顯示屏發送和接收指令。此漏洞可能允許攻擊者在未經許可的情況下遠端關閉播放器甚至關閉系統。

下圖顯示伺服器嘗試向 B1 顯示屏發送「Open Player」指令時捕獲的流量。

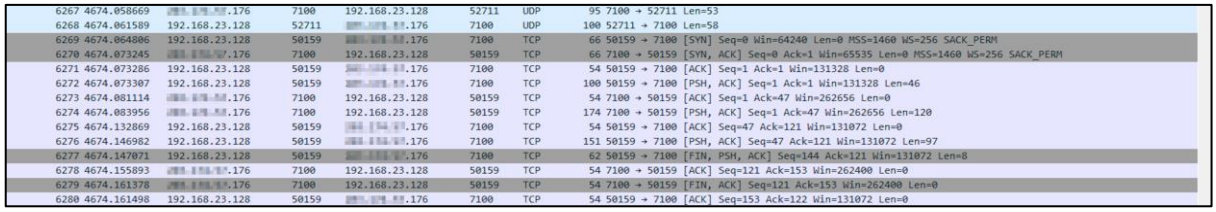

圖 13 - 伺服器嘗試向顯示屏發送 「Open Player」 指令時捕獲的流量

在伺服器向顯示屏發送指令之前，它會發送一個包含 「messagearrived>{UUID}」 的 UDP 數據包來通知顯示屏。顯示屏將使用 「replymessagearrived」 UDP 數據包回覆伺服器。

```
messagearrived>c6569916-3dae-49ff-88b1-aed76334d314

replymessagearrived>c6569916-3dae-49ff-88b1-aed76334d314
```

圖 14 - UDP 數據包的內容 A

顯示屏將與發送 UDP 數據包的 IP 地址建立 TCP 連接 (在圖 13 中，顯示屏伺服器的 IP 地址為「X.X.X.176」) 。然後，顯示屏發送一個 TCP 數據包，其中包含它之前收到的 UUID。伺服器將指令發送到顯示屏，當中 「transitType」 指定顯示屏需要執行的指令。顯示屏收到指令後，會將數據包發回伺服器確認收到後，再執行指令。

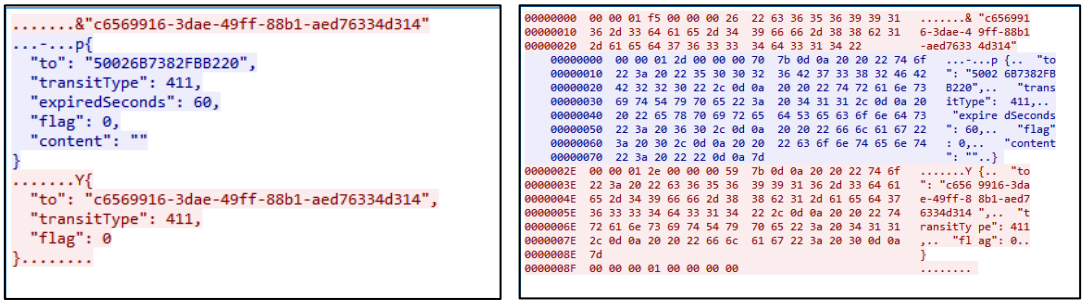

圖 15 - TCP 數據包 B 的內容

攻擊者可以假冒伺服器向顯示屏發送指令，首先發送 UDP 數據包，建立 TCP 連接，然後通過發送不同的 「transitType」 數值來請求操作。

由於 B1、C1 和 C2 顯示屏由同一軟件製造商製造的網頁管理平台管理，因此 B1、C1 和 C2 亦存在相同漏洞。

5.2.1.3. IoT-DEV-03： 暴露的外部介面埠

風險等級	高
受影響測試編號	A1、A2、B1、B2、C1、C2、D1、D2
OWASP IoT Top 10	I10：2018 - Lack of Physical Hardening

詳情

顯示屏背面存在幾個外部介面埠，包括 USB 埠、LAN 埠、HDMI 埠等。攻擊者可以利用這些埠執行各種攻擊，例如注入惡意 USB 快閃記憶體驅動器以顯示有害內容或關閉系統。

每個顯示屏上的外部介面埠數如下：

外部介面埠	***數碼顯示屏裝置測試編號***							
	A1	***A2***	***B1***	***B2***	***C1***	***C2***	***D1***	***D2***
電源開關	1	1	1	1	1	1	1	1
系統開關按鈕	1	0	1	0	1	0	1	0
USB 埠	1	1	2	2	4	2	2	1
LAN 埠	1	1	1	1	1	1	1	1
HDMI OUT 埠	0	0	0	0	1	0	0	0
HDMI IN 埠	0	0	0	0	0	*1* *	0	0
VGA 埠	0	0	0	0	1	0	0	0
音訊輸出埠	0	0	0	0	1	0	0	0

列表 5-3. 顯示屏裝置上的外部介面埠

* 由於連接的系統可以識別顯示屏的顯示器，所以 HDMI IN 連接埠運作正常。但是，無法更改顯示器的頻道以顯示連接的系統。

數碼顯示屏測試編號	照片
A1	
A2	
B1	
B2	
C1	 

C2		
D1		
D2		

列表 5-4. 顯示屏裝置上外部介面埠的照片

5.2.1.4. IoT-DEV-04： 啟用的觸控屏允許控制

風險等級	高
受影響測試編號	A1、A2、B1、B2、C1、C2
OWASP IoT Top 10	I10：2018 - Lack of Physical Hardening

詳情

所有顯示屏都允許用戶通過觸控與它們進行控制。一些顯示屏可以打開媒體播放器設定功能表，甚至通過執行特定的觸控手勢退出媒體播放器。

以下列表顯示退出媒體播放器/執行其他操作所需的觸控手勢：

數碼顯示屏裝置測試編號	手勢
A1	方法一：用手指從螢幕左邊緣滑動打開小部件->點擊「x」關閉播放器 方法二：用手指從螢幕右邊緣滑動以打開通知中心，這允許攻擊者打開設定
A2	用一根手指從螢幕底部邊緣滑動以顯示導航欄 - > 點擊主頁
B1	點擊螢幕右上角 5 次，打開播放器功能表 -> 退出
B2	長按螢幕 5 秒 ->出現「Please continue」提示 -> 按兩下五次以打開播放器選單-> 退出
C1	點擊螢幕右上角 5 次，打開播放器功能表 -> 退出
C2	點擊螢幕右上角 5 次，打開播放器功能表 -> 退出
D1	無法使用觸控手勢進行控制
D2	無法使用觸控手勢進行控制

列表 5-5. 退出媒體播放器/執行其他操作的手勢

5.2.1.5. IoT-DEV-05： 使用 USB 裝置顯示惡意程式

風險等級	高
受影響測試編號	*B1、C1*
OWASP IoT Top 10	I03：2018 - Insecure Ecosystem Interfaces

詳情

受影響的顯示屏具有允許它們將程式從 USB 快閃記憶體驅動器拉取到媒體播放器的功能。結合漏洞 IoT-DEV-03，如果攻擊者可以在 USB 快閃記憶體驅動器上創建有效的程式，則他們能夠執行惡意程式。

USB 快閃記憶體驅動器上的程式必須遵循特定的資料夾結構，攻擊者可以通過從伺服器下載程式時捕獲和分析顯示屏的流量來確定該結構。

5.2.2. 中等風險研究結果

5.2.2.1. IoT-DEV-06： 未加密的數據流量

風險等級	中等
受影響測試編號	A1、A2、B1、B2、C1、C2、D1、D2
OWASP IoT Top 10	I03：2018 - Insecure Ecosystem Interfaces I07：2018 - Insecure Data Transfer and Storage

詳情

所有顯示屏都沒有加密他們的數據流量。這允許攻擊者執行中間人 （MitM） 攻擊並窺探一些資訊，例如顯示屏中的圖像和視頻，甚至干擾流量以執行其他攻擊，例如 IoT-DEV-02。

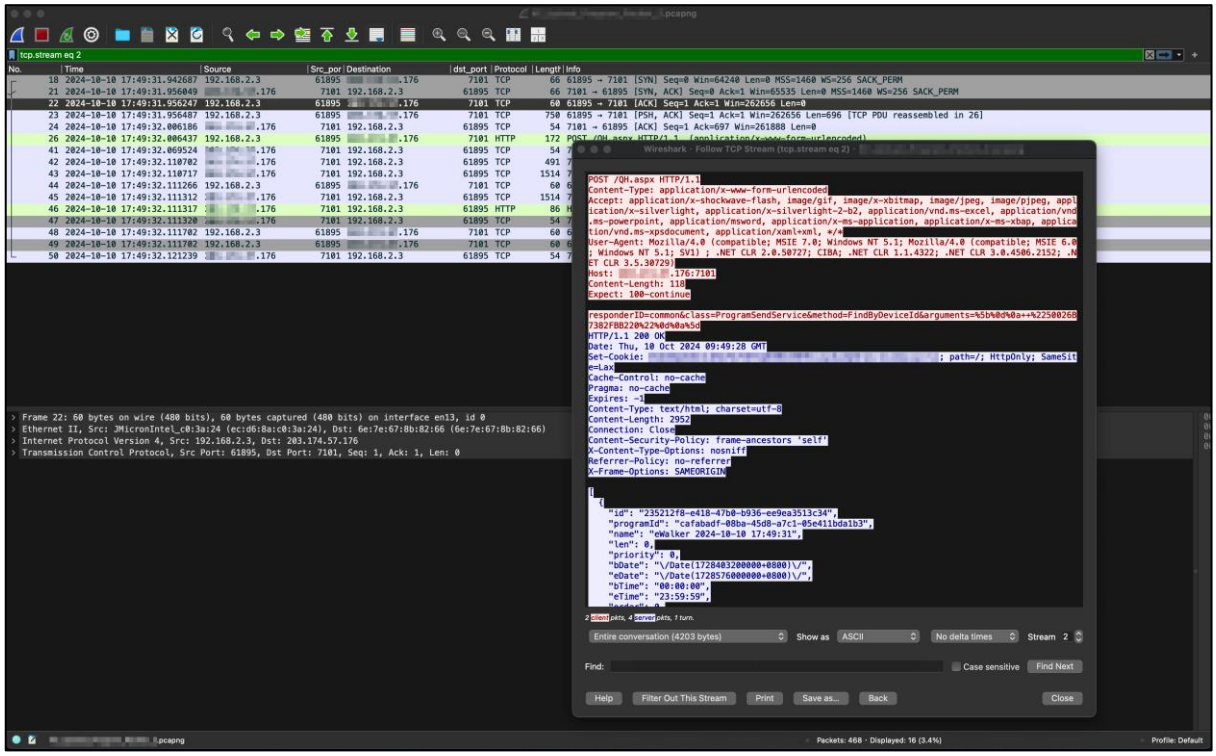

圖 16 - 包含程序內容的 TCP/HTTP 數據包

5.2.2.2. IoT-DEV-07： 停用 Windows 防火牆或 Windows Defender

風險等級	中等
受影響測試編號	*A1*、*D1*
OWASP IoT Top 10	I03：2018 - Insecure Ecosystem Interfaces I07：2018 - Insecure Data Transfer and Storage

詳情

A1 顯示屏預設停用 Windows 防火牆，而 *D1* 顯示屏預設不包含 Windows Defender。停用 Windows 防火牆後，顯示屏更容易受到未經授權的訪問。停用 Windows Defender 後，顯示屏更容易受到病毒、勒索軟件和其他惡意軟件的攻擊。

圖 17 - Windows 防火牆在 *A1* 顯示屏中被停用

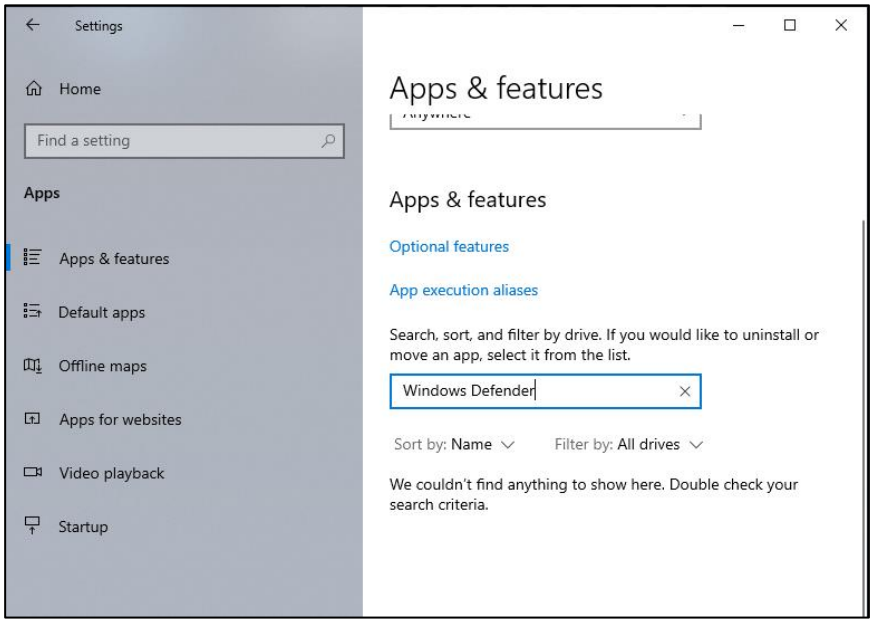

圖 18 - D1 顯示屏中未安裝 Windows Defender

5.2.3. 低風險研究結果

IoT-DEV-08： 阻斷服務（Denial of Service）

風險等級	低
受影響測試編號	A1、A2、B1、B2、C1、C2
OWASP IoT Top 10	I02：2018 - Insecure Network Services

詳情

當通過 LAN 連接/Wi-Fi 連接對目標顯示屏進行埠進行掃描時，顯示屏回應較為緩慢，導致用戶控制延遲。這指出阻斷服務（Denial of Service）攻擊(例如 TCP SYN Flood) 的潛在漏洞可能會耗盡其資源並使其不能運作或無法訪問。

5.2.3.1. IoT-DEV-09： 暴露了不必要的網絡服務

風險等級	低
受影響測試編號	A1、B1、C1、D1
OWASP IoT Top 10	I07：2018 - Insecure Data Transfer and Storage

詳情

一些顯示屏啟用了 Remote Procedure Calls(RPC)服務，網絡端口(Network Ports) 135 和 445 被開啟。這可能會增加通過這些網絡端口受到攻擊的風險。

6. 保安建議

根據此保安測試中的研究結果，本節提供有關應對和降低保安風險的建議。此外，數碼顯示屏用戶亦可以根據 HKCERT 的《物聯網數碼顯示屏保安指南》[3] 採用最佳保安實踐。

6.1. 顯示屏網頁管理平台上的保安建議

IoT-WEB-01 – 敏感數據洩露

- 通過身份驗證和授權實施嚴格的訪問控制措施，以確保只有授權用戶才能訪問敏感端點。
- 密碼和密碼雜湊不應反映在 API 回應中。

IoT-WEB-02 – 不安全的密碼雜湊

- 使用已建立的密碼雜湊演算法，例如 Argon2id、BCrypt 或 PBKDF2 並加入適當的參數。
- 在執行密碼雜湊時，在密碼雜湊中使用唯一的隨機密碼鹽（Password Salt），以提供更強的暴力破解防禦。萬一攻擊者獲得對相關資料庫的訪問權限，這會大大降低洩露用戶純文本密碼的機會。

IoT-WEB-03 – 過時的程式碼庫

- 定期檢查並更新供應商對程式碼庫的保安更新。

IoT-WEB-04 – SQL 注入

- 不要通過連接用戶輸入來建構 SQL 語句。
- 對所有變數使用參數化查詢。
- 使用白名單方法實施嚴格的輸入驗證，以確保用戶輸入符合預期標準。
- 通過顯示隱藏資料庫和應用程式邏輯詳細資訊的一般錯誤來避免暴露詳細的 SQL 錯誤消息。

IoT-WEB-05 – 訪問控制失效

- 確保只有具有必要權限的授權用戶才能訪問關鍵功能，例如系統重啟和管理平台的 URL 連結。
- 應嚴格限制普通用戶使用其分配的權限。

IoT-WEB-06 – 繞過客戶端驗證

- 確保在伺服器端驗證所有輸入（包括「email」等參數）。

IoT-WEB-07 – 跨網站指令碼

- 實施伺服器端清理步驟以清除用戶提供的內容。
- 驗證上傳檔案的內容類型，以確保它們與預期格式相符
- 實施較安全的內容保安策略 （Content Security Policy - CSP） 以限制內聯 JavaScript 的執行和未經授權的外部資源的載入。

IoT-WEB-08 – 固定通訊

- 確保通訊令牌在每次成功登入、登出或任何保安上下文更改時更改。

IoT-WEB-09 – 未經身份驗證可以訪問的檔案

- 實施適當的訪問控制，以確保只有具有適當權限並經過身份驗證的用戶才能訪問上傳的檔。
- 將檔案儲存在受保護的目錄或公共網頁目錄之外，的過身份驗證的訪問路由來通過驗證用戶通訊後提供服務。

IoT-WEB-10 – 更改密碼不需要重新身份驗證

- 更改密碼時驗證當前密碼。

IoT-WEB-11 – 不安全的 HTTP 使用

- 通過實施 SSL/TLS 並將 HTTP 流量重新導向到 HTTPS，將伺服器設定為使用 HTTPS 進行所有通訊
- 啟用 HTTP Strict Transport Security （HSTS） 以對所有未來的通訊強制實施 HTTPS，從而自動將用戶從 HTTP 重新導向到 HTTPS。

6.2. 顯示屏裝置上的保安建議

IoT-DEV-01 – 通過紅外線進行未經授權的控制

- 如果不需要紅外線功能，通過拔下電線或使用膠帶或其他材料擋住紅外線感測器來停用紅外感測功能。

IoT-DEV-02 – 未經授權向顯示屏發送指令

- 加密伺服器和數碼顯示屏裝置之間的通訊。
- 設定顯示屏以驗證數據包的來源，以確保指令來自合法的伺服器。
- 在指令數據包中包含記錄時間和隨機數以防止重放攻擊。
- 通過創建防火牆規則，阻止來自未知 IP 地址的惡意數據包，並且僅允許來自合法顯示屏伺服器的數據包。

IoT-DEV-03 – 公開的外部介面埠

- 通過添加物理鎖來限制對外部介面埠 (如 USB 埠、HDMI 埠和網絡埠) 的物理訪問。

IoT-DEV-04 – 啟用觸控屏允許控制

- 停用觸控功能：

對於 Windows 顯示屏，用戶可以通過以下步驟停用「HID 相容觸控屏」來停用觸控功能：

1. 按「Windows」鍵 + 「X」。選擇「裝置管理員」
2. 在「人體學介面裝置」下，找到「HID Compliant Touchscreen」
3. 右鍵按下裝置名稱並選擇 「停用」

對於 Android 顯示屏，用戶可以固定應用程式的螢幕以保持其可見狀態，直到用戶使用您的 PIN、圖案或密碼取消固定它。 他們必須先通過以下步驟開啟「App 螢幕固定」：

1. 打開顯示屏的 Settings 應用程式
2. 點擊「安全性」或「安全性和位置」>「高級」>「App 螢幕固定」

3. 開啟「App 螢幕固定」

然後，用戶可以通過以下步驟固定應用程式：

1. 轉到媒體播放器應用程式
2. 點擊 「總覽」打開概覽
3. 在圖像頂部，點按應用程式的圖示
4. 點擊「固定」

如果需要觸控功能，供應商應鎖定程式或停用某些作業系統手勢，以確保攻擊者無法退出媒體播放器。此外，供應商可以執行作業系統強化以限制允許執行的程式。

IoT-DEV-05 – 使用 USB 裝置顯示惡意程式

- 通過停用通過系統訪問或添加物理鎖 (例如 USB 埠、HDMI 埠、網絡埠等) 來限制對外部介面的物理訪問。

IoT-DEV-06 – 未加密的數據流量

- 加密伺服器和數碼顯示屏裝置之間的通訊。

IoT-DEV-07 – 停用了 Windows 防火牆/Windows Defender

- 安裝並啟用 Windows 防火牆和 Windows Defender。

IoT-DEV-08 – 阻斷服務 （Denial of Service）

- 將流量限制應用於特定顯示屏並檢測非法流量，並通過設定路由器/交換器在路由等級上阻止它。

IoT-DEV-09 – 暴露了不必要的網絡服務

- 停用不需要網絡服務，或使用網絡防火牆阻止其網絡訪問。

7. 引用

[1] https://owasp.org/Top10/
[2] https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Top_10
[3] https://www.hkcert.org/tc/security-guideline/iot-security-guideline-for-digital-signage