TAICS

TAICS TS-0047 v1.0 : 2022

# 機上盒資安標準

# Cybersecurity standard for set-top boxes

2022/06/30

社團法人台灣資通產業標準協會
Taiwan Association of Informationand Communication Standards

# 機上盒資安標準

# Cybersecurity standard for set-top boxes

出版日期: 2022/06/30

終審日期: 2022/03/29

# 誌謝

本標準由台灣資通產業標準協會－TC5 網路與資訊安全技術工作委員會所制定。

TC 主席：神盾股份有限公司 張心玲 副總經理

TC 副主席：財團法人電信技術中心 林炫佑 副執行長

TC 副主席：財團法人資訊工業策進會 蔡正煜 主任

TC 物聯網資安工作組組長：財團法人資訊工業策進會 高傳凱 副主任

技術編輯：財團法人電信技術中心 許博堯 副理、吳宗恩 工程師

此標準制定之協會會員參與名單為(以中文名稱順序排列)：

中華資安國際股份有限公司、中華電信股份有限公司、台灣是德科技股份有限公司、安華聯網科技股份有限公司、亞太電信股份有限公司、社團法人台灣數位電視協會、神盾股份有限公司、財團法人工業技術研究院、財團法人台灣商品檢測驗證中心、財團法人資訊工業策進會、財團法人電信技術中心、國立陽明交通大學、耀登科技股份有限公司

本計畫專案參與廠商(法人)名單為(以中文名稱順序排列)：

國家通訊傳播委員會、台灣數位光訊科技股份有限公司、國立雲林科技大學

本標準由國家通訊傳播委員會支持研究制定

# 目錄

# 前言

本標準係依台灣資通產業標準協會(TAICS)之規定，經理事會審定，由協會公布之產業標準。

本標準並未建議所有安全事項，使用本標準前應適當建立相關維護安全與健康作業，並且遵守相關法規之規定。

本標準之部分內容，可能涉及專利權、商標權與著作權，協會不負責任何或所有此類專利權、商標權與著作權之鑑別。

# 引言

數位經濟是國家發展之重要課題，其安全與可信賴的通傳網路則是重要之基礎，而機上盒屬於通傳網路用戶終端設備，也屬於通傳網路中的一環，除有線電視業者與多媒體隨選視訊服務(MOD)業者提供之機上盒，近年來亦有諸多以行動作業系統為基礎之 OTT(Over the Top, OTT)機上盒。用戶可使用內建或自行安裝影音視訊服務(如：Netflix、CatchPlay、HBO GO)，伴隨連網功能與應用日趨多元，包括影視服務、網購服務等，以致資安威脅相應而生。

以 CVE 漏洞為例，2020 年，由於機上盒可透過 Telnet 遠端服務於機器啟動時連帶開啟服務，攻擊者則可透過此服務連線進入機上盒系統存取系統儲存之敏感性資料；或機上盒使用未加密的方式通訊，導致攻擊者可惡意修改資訊，給予使用者錯誤訊息，甚至進行惡意詐騙或勒索威脅等惡意行為。又如 2021 年被發現機上盒存在訊息洩漏風險，該風險源於設備未對日誌進行身分驗證，攻擊者可利用該風險獲取使用者敏感性資料，甚至更進一步的攻擊。

基此，國家通訊傳播委員會(National Communications Commission, NCC)為確保機上盒之安全性，委託財團法人電信技術中心(Telecom Technology Center, TTC)參考國際標準、規範與指引，在台灣資通產業標準協會(Taiwan Association of Information and Communication Standards, TAICS)標準制定平臺，聚集產、官、學、研，依產業標準制定程序，進行機上盒資安標準之制定。後續除將建立產品認驗證制度，推動機上盒符合資安標準規範，以保障消費者的使用安全之外，同時協助產業提升資安能力及產品競爭力。

# 1. 適用範圍

本標準規定機上盒之資訊安全要求。機上盒是透過連接天線、衛星、同軸電纜、有線或無線網路，以接收並解調固定通信多媒體內容傳輸平臺、有線廣播電視系統及網際網路視聽服務平臺傳送之訊號，提供客戶端影視服務之終端設備。

適用範圍為機上盒本體，包含硬體、韌體、輸出入接口、傳輸協定、系統服務、出廠內建軟體、使用者在機上盒輸入的敏感性資料，及操作的訂閱繳費等金流活動。

不具備網路連線功能之機上盒設備、僅透過 APP 等軟體功能提供影視服務之行動裝置與個人電腦設備、影音內容保護及使用者額外安裝之 APP 與應用程式不在本標準規範之範圍。

適用範圍如圖 1 紅框所示。

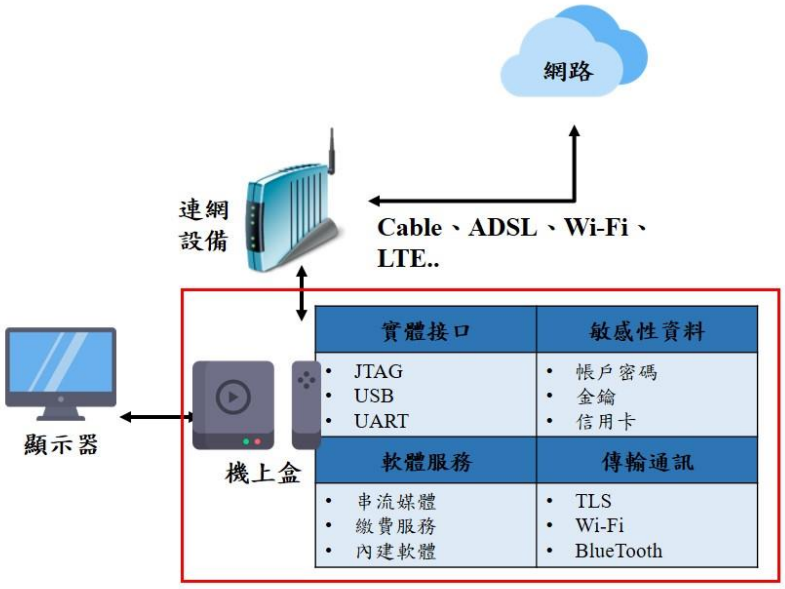


圖 1 適用範圍示意圖

# 2. 引用標準

下列標準因本標準所引用，成為本標準之一部分。有加註年份者，適用該年份之版次，不適用於其後之修訂版(含補充增修)。無加註年份者，適用其最新版(含補充增修)。

[1] NIAP，Collaborative Protection Profile for Network Devices_V2.1：2019

[2] ITU-T，H.721 IPTV terminal devices: Basic model：2016

[3] CableLabs，Requirements CPE Security Common Security Requirements for IP-Based MSO-Provided CPE_V01：2013

[4] 國家通訊傳播委員會：資通安全指引 ISG012 - 具網際網路連線功能之固定通信多媒體內容傳輸平臺及有線廣播電視機上盒資通安全檢測技術指引：2019

[5] 台灣資通產業標準協會：TAICS TS-0045 v1.0:2021 - 消費性物聯網產品資安標準：2021

[6] 台灣資通產業標準協會：TAICS TS-0029 v1.0:2020 - 智慧型手機系統內建軟體資安標準：2020

# 3. 用語及定義

下列用語及定義適用於本標準。

## 3.1 加密(Encryption)

指明文資訊透過加密數學演算法進行改變，使改變後的資料不具可讀性，而接收端用相對應之解密數學演算法可以恢復明文資訊而達到保密的目的。

## 3.2 通訊埠(Port)

通訊埠，又稱為網路埠或連接埠。內建軟體因服務需求開啟，作為連網裝置與外部傳送/接收通訊資料。

## 3.3 敏感性資料(Sensitive Data)

指洩漏時導致使用者造成損害之資料，包括但不限於個人資料、通行碼、金鑰或地理位置等。此等資料依使用者行為或應用程式之運作，於裝置及其附屬儲存媒體建立、儲存或傳輸。

## 3.4 通行碼(Password)

通行碼(或被稱為密碼)指的是一組字元串，通常用於保護隱私資訊及防止未經授權之操作，可用以確認使用者之身分。

## 3.5 常見漏洞評鑑系統(Common Vulnerability Scoring System, CVSS)

指一套漏洞評鑑系統的判定標準，包括威脅所造成損害的嚴重性、資安脆弱性的可利用程度與攻擊者不當運用該脆弱性的難易度，都被列入計分。自 0 分至 10 分，0 代表無風險，10 則代表最高風險。在此標準內 CVSS 分數以具有最新版本之評定分數為判定標準。

### 3.6 安全等級(Security Level)

指因應產品面臨不同程度之資安威脅，針對產品所需的安全功能要求提供不同強度之分級。

### 3.7 多因子鑑別(Multi-Factor Authentication, MFA)

指採用 2 種以上因子的鑑別機制，以獲得裝置之存取權限。多因子鑑別依據 3 個因子，包括所知之事(something you know)、所持之物(something you have)、所具之形(something you are)，於不同階段對同一裝置進行鑑別。

### 3.8 強鑑別(Strong Authentication)

指使用者在登入過程中，要求使用者針對登入詢問輸入獨一無二的單次回應，或輸入由驗證伺服器提供的特殊代碼，使用者必須使用特殊的硬體或軟體 Token，對詢問提供正確的回應。現今驗證協議有 FIDO（Fast IDentity Online）：通用鑑別框架（Universal Authentication Framework, UAF）、通用第二因子（Universal Second Factor, U2F）與 FIDO2/WebAuthn。

### 3.9 內建軟體(Embedded Software)

指機上盒製造商於出廠時即安裝於機上盒內之軟體，包含系統內之有圖示與無圖示軟體，使用者自行安裝的軟體則不在此範圍內。

### 3.10 金鑰(Key)

指為了驗證、鑑別、加密或解密之目的，而與演算法結合使用之參數。

### 3.11 關鍵安全參數(Critical Security Parameters)

係指與安全相關之資料(例如:機密資訊、金鑰)及身分驗證資料（例如:通行碼、PIN 碼），當此資料被揭露或修改時，可能會損害密碼模組的安全性。如：產品透過 OTA 更新韌體時，更新伺服器發送之憑證金鑰遭惡意人士竄改或擷取，可能造成更新失敗或韌體遭竊取。

## 3.12 作業系統保護區(Operating System Protection Area)

指使用者透過外部裝置連接機上盒，在管理者權限下可存取之空間，包含機上盒本身儲存空間。反之，非作業系統保護區則是在非管理者權限下可存取之空間。

## 3.13 個人資料(Personal Data)

指含自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料[6]。

## 3.14 持久性儲存器(Persistent Storage)

指此類的儲存設備所儲存的任何資料，在該設備電源關閉後資料仍會保存。亦稱為非揮發性記憶體(Non-volatile storage)，例如:唯讀記憶體(ROM)、快閃記憶體(flash)、硬碟(hard disk)等。

# 4. 安全等級

安全等級係為降低或消弭產品之資訊安全威脅，透過最適之安全組合，確保產品達到安全之要求。本標準安全等級 1、2、3 分別對應至「機上盒資安測試規範」安全等級 1、2、3 之安全要求。

## 4.1 安全等級概述

### 4.1.1 安全等級說明

安全等級依據 MITRE ATT&CK 入侵攻擊流程，機上盒可能被入侵的路徑、漏洞評鑑系統(CVSS)的漏洞評分機制、與參考具網際網路連線功能之固定通信多媒體內容傳輸平臺及有線廣播電視機上盒資通安全檢測技術指引，所訂定的安全等級，將檢測標準區分 1 級、2 級、3 級三個等級。

1 級安全要求所對應為檢測機上盒，是否未將其本身資訊進行加密保護，易於攻擊者取得資訊，以及存在高風險之漏洞。

2 級安全要求所對應為針對發現的漏洞、系統服務等資訊，進行初步測試，檢視是否可被利用，以及機上盒內建軟體之安全。

3 級安全要求所對應為檢測機上盒是否具備相關的防護機制，核心內部資訊加密之標準是否採用國際通用標準，其對應之列即其所應通過的安全要求分項，安全等級越高，其涵蓋範圍與要求也越嚴謹。

### 4.1.2 安全構面

(a) 可用性：主要包含機上盒網路傳輸技術及通訊協定等安全要求，並確保功能服務提供的穩定性。

(b) 身分識別：主要包含機上盒對於通行碼設定、登入介面的防護機制與使用權限的安全要求。

(c) 隱私加密：主要包含機上盒資料的保護，在傳輸通訊的資料，或是儲存在設備上敏感性資料的加密機制。

(d) 安全功能：主要包含機上盒的安全機制，預設的功能設定、本身系統的已知弱點或使用不安全的第三方套件。

### 4.1.3 安全要求分項

依安全構面所設計對應之安全要求要項，且每一安全要求分項包含一個以上之安全要求，如表 1 所示，第一欄為安全構面，包括：(1)可用性、(2)身分識別、(3)隱私加密、(4)安全功能；第二欄為安全要求分項，係依各安全構面設計對應之安全要求；第三欄為安全等級，按各安全要求分項之驗證結果，作為安全等級評估標準。其對應之列即其所應符合的安全要求分項，安全等級級數的大小代表安全等級的高低，欲符合較高等級之安全要求應先滿足較低安全等級要求。本安全等級總表各欄的關連性，須依循下節 5.1 至 5.4 之技術規範內容。

表 1 安全等級總表

| 安全構面 | 安全要求分項 | 安全等級 | | |
|---|---|---|---|---|
| | | 1 級 | 2 級 | 3 級 |
| 5.1 可用性 | 5.1.1 系統更新 | 5.1.1.1<br>5.1.1.2<br>5.1.1.3 | - | - |
| | 5.1.2 Wi-Fi 及藍牙模糊測試 | - | 5.1.2.1<br>5.1.2.2 | - |
| | 5.1.3 安全性回報 | 5.1.3.1 | - | - |
| 5.2 身分識別 | 5.2.1 工程模式 | 5.2.1.1 | - | - |
| | 5.2.2 付費功能身分識別 | - | - | 5.2.2.1 |
| 5.3 隱私加密 | 5.3.1 登入保密功能 | 5.3.1.1 | - | - |
| | 5.3.2 最小化通訊埠 | 5.3.2.1 | - | - |
| | 5.3.3 資料傳輸 | 5.3.3.1<br>5.3.3.2 | 5.3.3.3 | - |
| | 5.3.4 敏感性資料存取 | 5.3.4.1<br>5.3.4.2 | - | - |
| | 5.3.5 資料紀錄刪除 | 5.3.5.1 | - | - |

| 安全構面 | 安全要求分項 | 安全等級 | | |
|---|---|---|---|---|
| | | 1 級 | 2 級 | 3 級 |
| | 5.3.6 資料儲存保護 | 5.3.6.1 | 5.3.6.2<br>5.3.6.3<br>5.3.6.4 | - |
| 5.4 安全功能 | 5.4.1 作業系統常見漏洞 | 5.4.1.1 | 5.4.1.2 | 5.4.1.3 |
| | 5.4.2 實體埠安全 | - | 5.4.2.1 | 5.4.2.2 |
| | 5.4.3 敏感性資料儲存 | - | - | 5.4.3.1<br>5.4.3.2<br>5.4.3.3<br>5.4.3.4 |
| | 5.4.4 Wi-Fi 網路熱點 | 5.4.4.1 | - | - |
| | 5.4.5 內建軟體安全 | - | 5.4.5.1 | 5.4.5.2<br>5.4.5.3 |

# 5. 標準規範

本節詳盡載明機上盒可用性、身分識別、隱私加密、安全功能應採取之測試項目，所有機上盒應符合本節中所有安全要求。

## 5.1 可用性

### 5.1.1 系統更新

5.1.1.1 機上盒應支援更新功能。

5.1.1.2 機上盒進行系統更新後，用戶設定應與更新前相符。

5.1.1.3 機上盒更新服務應使用 TLS 1.2(含)以上之國際標準安全加密通道傳輸。

### 5.1.2 Wi-Fi 及藍牙模糊測試

5.1.2.1 機上盒 Wi-Fi 傳輸應具有抗異常封包格式之保護機制。

5.1.2.2 機上盒藍牙傳輸應具有抗異常封包格式之保護機制。

### 5.1.3 安全性回報

5.1.3.1 機上盒應具備安全性回報之機制。

## 5.2 身分識別

### 5.2.1 工程模式

5.2.1.1 機上盒工程模式通行碼應為 8 字元(含)以上。

### 5.2.2 付費功能身分辨識

5.2.2.1 機上盒服務與內建軟體付費功能應使用多因子鑑別或強鑑別進行用戶身分辨識。

## 5.3 隱私加密

### 5.3.1 登入保密功能

5.3.1.1 機上盒進行通行碼輸入時，應以特殊字元進行遮蔽。

### 5.3.2 最小化通訊埠

5.3.2.1 機上盒系統與服務應關閉非必要使用的通訊埠及遠端存取服務。

### 5.3.3 資料傳輸

5.3.3.1 機上盒 OTT 服務應使用 TLS 1.2(含)以上之國際標準安全加密通道傳輸。

5.3.3.2 機上盒付費功能應使用 TLS 1.2(含)以上之國際標準安全加密通道傳輸。

5.3.3.3 機上盒內建軟體付費功能應使用 TLS 1.2(含)以上之國際標準安全加密通道傳輸。

### 5.3.4 敏感性資料存取

5.3.4.1 機上盒服務與內建軟體存取敏感性資料時，應提供隱私權政策或使用聲明。

5.3.4.2 機上盒內建軟體開啟之權限，應與使用者同意開啟之權限一致。

### 5.3.5 資料記錄刪除

5.3.5.1 機上盒應具備可刪除使用者資料紀錄之機制。

### 5.3.6 資料儲存保護

5.3.6.1 機上盒提供使用者之紀錄或日誌，不應將敏感性資料以明文顯示。

5.3.6.2 機上盒內建軟體應將帳號、通行碼或金鑰儲存於作業系統保護區內或以加密方式儲存。

5.3.6.3 機上盒內建軟體不應將帳號、通行碼或金鑰以明文方式存在於執行檔中。

5.3.6.4 機上盒內建軟體不應在執行期間將敏感性資料明文儲存於系統日誌中。

## 5.4 安全功能

### 5.4.1 作業系統常見漏洞

5.4.1.1 機上盒作業系統不應存有 CVSS 評分 9.0(含)以上的已知漏洞。

5.4.1.2 機上盒作業系統不應存有 CVSS 評分 7.0(含)以上的已知漏洞。

5.4.1.3 機上盒作業系統不應存有 CVSS 評分 4.0(含)以上的已知漏洞。

### 5.4.2 實體埠安全

5.4.2.1 機上盒不得透過實體介面直接進入作業系統之除錯模式。

5.4.2.2 機上盒應具備紀錄內部系統登入登出之日誌機制。

### 5.4.3 安全敏感性資料儲存

5.4.3.1 機上盒持久性儲存器內之關鍵安全參數應具備保護機制。

5.4.3.2 機上盒產品唯一識別碼應具備防篡改之機制。

5.4.3.3 機上盒韌體檔內之關鍵安全參數應具備保護機制。

5.4.3.4 機上盒更新及關連服務間傳輸之關鍵安全參數應具備唯一性。

### 5.4.4 Wi-Fi 網路熱點

5.4.4.1 機上盒開啟熱點時應提供 WPA2 以上加密通訊協定且應允許設定高複雜性之通行碼機制。

### 5.4.5 內建軟體安全

5.4.5.1 機上盒內建軟體之執行檔不應存有 CVSS 評分 7.0(含)以上的已知漏洞。

5.4.5.2 機上盒內建軟體可輸入之欄位應具備防護注入攻擊之機制。

5.4.5.3 機上盒內建軟體之執行檔應具備反編譯防護機制。

# 附錄 A
# (參考)
# 標準規範要求事項與各標準規範對照

表 A.1 標準規範要求事項與各標準規範對照表

| 本標準要求事項 | 參考或對應標準規範 |
|---|---|
| 5.1.1 系統更新 | 消費性物聯網產品資安標準(5.3.1.1、5.3.1.2、5.3.1.7、5.3.1.10) |
| 5.1.2 Wi-Fi 及藍牙模糊測試 | 具網際網路連線功能之固定通信多媒體內容傳輸平臺及有線廣播電視機上盒資通安全檢測技術指引(7.2.2) |
| 5.1.3 安全性回報 | 具網際網路連線功能之固定通信多媒體內容傳輸平臺及有線廣播電視機上盒資通安全檢測技術指引(7.3.5、7.3.6、7.3.7) |
| 5.2.1 工程模式 | 智慧型手機系統內建軟體資安標準(7.2.4) |
| 5.2.2 安全功能設定 | 具網際網路連線功能之固定通信多媒體內容傳輸平臺及有線廣播電視機上盒資通安全檢測技術指引(7.2.4) |
| 5.2.3 付費功能身分識別 | 消費性物聯網產品資安標準(5.4.2.5) |
| 5.2.4 記錄日誌身分辨識 | CVE-2021-21722 |
| 5.3.1 登入保密功能 | 智慧型手機系統內建軟體資安標準(5.1.4.2) |
| 5.3.2 最小化通訊埠 | CVE-2020-11618<br>具網際網路連線功能之固定通信多媒體內容傳輸平臺及有線廣播電視機上盒資通安全檢測技術指引(7.2.3、7.3.1) |
| 5.3.3 資料傳輸 | CVE-2020-11617<br>具網際網路連線功能之固定通信多媒體內容傳輸平臺及有線廣播電視機上盒資通安全檢測技術指引(7.2.1) |
| 5.3.4 敏感性資料存取 | 消費性物聯網產品資安標準(5.2.2.1) |
| 5.3.5 使用者資料紀錄 | 智慧型手機系統內建軟體資安標準(5.1.6.3) |
| 5.3.6 內建軟體資料儲存保護 | 具網際網路連線功能之固定通信多媒體內容傳輸平臺及有線廣播電視機上盒資通安全檢測技術指引(7.2.5) |
| 5.4.1 作業系統漏洞 | 消費性物聯網產品資安標準(5.4.2.1) |
| 5.4.2 實體埠安全 | 具網際網路連線功能之固定通信多媒體內容傳輸平臺及有線廣播電視機上盒資通安全檢測技術指引(7.4.2) |
| 5.4.3 敏感性資料儲存 | 消費性物聯網產品資安標準(5.7.1.8) |
| 5.4.4 Wi-Fi 網路熱點 | 消費性物聯網產品資安標準(5.7.1.4) |
| 5.4.5 內建軟體安全 | CVE-2018-14989<br>智慧型手機系統內建軟體資安標準(5.1.2.1) |

# 附錄 B
# (參考)
# 風險來源分析與資安需求

表 B.1 風險來源分析與資安需求表

| 威脅描述 | 威脅目標 | 攻擊技術 | 防護對策 | 安全構面 |
|---|---|---|---|---|
| 除錯模式無身分鑑別 | 系統存取權敏感性資料 | 藉由 JTAGUART 等除錯介面取得系統存取權 | 移除除錯介面<br>加上身分鑑別 | 安全功能 |
| | 參考來源:DEF CON 26 Breaking Smart Speaker - Exploit Amazon Echo<br>https://github.com/tencentbladeteam/Exploit-Amazon-Echo | | | |
| 韌體無更新機制 | 系統存取權<br>敏感性資料 | 竄改韌體取得<br>系統存取權 | 防止韌體遭到竄改 | 可用性 |
| | 參考來源：ENISA Baseline Security Recommendations for IoT<br>https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot | | | |
| 韌體無正確性與完整性檢查機制 | 系統存取權<br>敏感性資料 | 系統存取權<br>敏感性資料 | 防止韌體遭到竄改 | 可用性 |
| | 參考來源：Trend Micro, The Sound of a Targeted Attack<br>https://documents.trendmicro.com/assets/pdf/The-Sound-of-a-Targeted-Attack.pdf | | | |
| 不安全儲存位置 | 敏感性資料 | 資料爬蟲 | 存放於作業系統保護區 | 隱私加密 |
| | 參考來源：<br>DEFCON 2018: Vulnerable Out of the Box - An Evaluation of Android Carrier Devices | | | |
| 第三方函式庫漏洞 | 系統軟體 | 利用已知漏洞 | 已知漏洞修補 | 安全功能 |
| | 參考來源：<br>A Pattern for Remote Code Execution using Arbitrary File Writes and MultiDex Applications | | | |
| 隨意讀取機上盒資料 | 敏感性資料 | 未經授權讀取資料 | 敏感性資料使用前取得使用者同意 | 隱私加密 |
| | 參考來源：<br>A Pattern for Remote Code Execution using Arbitrary File Writes and MultiDex Applications | | | |
| 注入式攻擊 | 資料庫、取得使用者之權限 | Injection 攻擊 | 提供注入攻擊防護 | 安全功能 |
| | 參考來源：APP 軟體問題導致任意訊息發送、SQL Injection 等多個漏洞 | | | |
| 惡意修改通訊協定傳輸格 | 裝置可用性 | 修改通訊協定傳輸格式 | 模糊測試 | 可用性 |
| | 參考來源：Smartphone Secure Development Guidelines | | | |
| 傳輸資訊截取修改 | 通訊資料 | 中間人 | 提供信任傳輸通道 | 隱私加密 |
| | 參考來源：機上盒應用程式開發上被忽略的 SSL 處理 | | | |

# 參考資料

(1) SSLlabs，SSL and TLS Deployment Best Practices：2020

(2) NIST SP 800-124 Rev 1, Guidelines for Managing the Security of Mobile Devices in the Enterprise：2013

(3) NIST SP 800-164 DRAFT, Guidelines on Hardware-Rooted Security in Mobile Devices：2012

(4) NIST SP 800-163, Vetting the Security of Mobile Applications：2015

(5) NIST FIPS PUB 140-2, Security Requirements For Cryptographic Modules：2001

(6) 個人資料保護法 https://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=I0050021

(7) Department of Homeland Security (DHS), Study on Mobile Device Security：2017

(8) ETSI TS 103 645 V1.1.1 (2019-02), CYBER; Cyber Security for Consumer Internet of Things.

(9) NISTIR 8259 Draft (2nd) Recommendations for IoT Device Manufacturers: Foundational Activities and Core Device Cybersecurity Capability Baseline.

(10) NIST，National Vulnerability Database, https://nvd.nist.gov/vuln/full-listing

(11) NIST，SP 800-140C, CMVP Approved Security Functions, available at URL: https://csrc.nist.gov/projects/cryptographic-module-validation-program

(12) FIRST, Common Vulnerability Scoring System version 3.1: Specification Document, https://www.first.org/cvss/specification-document

(13) NIST Special Publication 800-57: Recommendation for Key Management, https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final

(14) ENISA，Cybersecurity Certification: EUCC Candidate Scheme v1：2020。

(15) OWASP，Mobile Security Project - Top Ten Mobile Risks：2016

(16) NIST，SP 800-53 Rev.5，Security and Privacy Controls for Information Systems and Organizations：2020。

(17) 政府組態基準(GCB)，TWGCB-01-004_Microsoft Windows 8.1 政府組態基準說明文件 v1.6：2020。

# 版本修改紀錄

| 版本 | 時間 | 摘要 |
|---|---|---|
| v1.0 | 2022/06/30 | 出版 |
| | | |
| | | |
| | | |
| | | |


地　址・台北市中正區北平東路30-2號6樓
電　話・+886-2-23567698
Email・secretariat@taics.org.tw
www.taics.org.tw