行動通信增波器

資通安全檢測技術指引

中華民國 109 年 2 月 18 日

目　次

行動通信增波器資通安全檢測技術指引

1. 前言

為確保行動通信網路之資通安全，爰訂定本指引。

2. 適用範圍

本指引適用於行動通信增波器。

3. 引用標準

本指引參考標準如下：

3.1 CNS 15408。

3.2 行政院國家資通安全會報技術服務中心，政府組態基準 Microsoft Windows 8.1（V1.4）。

3.3 NIST Special Publication 800-121 Revision 2, Guide to Bluetooth Security. June 2012. May 8, 2017。

3.4 DHS 4300A Sensitive Systems Handbook：Attachment Q6 Bluetooth Security。

3.5 無線區域網路接取設備及路由設備資通安全檢測技術指引。

3.6 影像監控系統資安標準—第一部：一般要求，Version 1.0，2018/06，台灣資通產業標準協會。

3.7 ETSI TS 133 117 V14.1.0 （2017-05）, Universal Mobile Telecommunications System （UMTS）； LTE；Catalogue of general security assurance requirements （3GPP TS 33.117 version 14.1.0 Release 14）。

3.8 OWASP IOT TOP 10 -2018。

4. 用語及定義

4.1 增波器

指行動通信基地臺與用戶終端設備間提供上下行鏈路接收、放大及發送射頻載波之設備。

4.2 韌體 （Firmware）

指嵌入在硬體裝置中的軟體。主要是將程式碼或資料寫入在唯讀記憶體內。指待測物實現安全功能需求對外溝通之介面。

4.3 美國國家脆弱性資料庫 （National Vulnerability Database）

指美國國家標準技術研究所（National Institute of Standards and Technology，NIST）提供的國家脆弱性資料庫，負責常見脆弱性與曝露之資料的發布及更新。

4.4 共同脆弱性與曝露 （Common Vulnerability and Exposures， CVE）

指美國國土安全部贊助之脆弱性管理計畫，該計畫針對每一脆弱性項目賦予其全球認可唯一共同編號。

4.5 共同脆弱性計分系統（Common Vulnerability Scoring System ，CVSS）

為一套共同脆弱性計分系統的判定標準，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，而 10 則代表最高風險。

5. 測試項目、方法及合格標準

測試項目包括實體安全、系統安全、通訊安全、身分鑑別與授權機制安全，申請人應配合提供設備概述等測試所需資訊（詳附表）及未加密韌體。

5.1 實體安全

5.1.1 實體防拆保護測試

5.1.1.1 測試方法

檢視待測物外殼有無防拆設計。

5.1.1.2 合格標準

待測物外殼應採一體成形(非零件組合而成)或使用防拆螺絲(採特殊頭型及沖針設計，一般十字或一字起子無法拆卸）等降低外殼遭拆除之設計。

5.1.2 實體介面安全管控測試

5.1.2.1 測試方法

透過實體埠連接待測物。

5.1.2.2 合格標準

符合下列任一項目即通過：

（1）預設將除錯介面（Debug Interface）從印刷電路板（Printed Circuit Board）上移除。

（2）除錯模式（Debug Mode）功能預設關閉。

（3）可透過實體埠存取待測物資訊者，存取前應通過鑑別機制，且鑑別機制應符合 5.4 身分鑑別與授權機制安全規定。

5.1.3 電源中斷恢復測試

5.1.3.1 電源中斷恢復測試

中斷電源供應。

5.1.3.2 合格標準

電力恢復後，系統恢復正常運作。

5.2 系統安全

5.2.1 事件紀錄測試

5.2.1.1 測試方法

（1）登入待測物管理頁面。

（2）設定並啟動待測物之事件紀錄功能。

（3）變更任一系統設定值並套用。

（4）清除事件紀錄。

（5）登出、登入及以錯誤方式登入。

（6）中斷待測物行動通信上鏈鏈路。

5.2.1.2 合格標準

測試方法（3）至（6）執行後，待測物應產出相關紀錄，且包括下列資訊：

（1）事件發生日期及時間。

（2）事件觸發者。

（3）事件類別。

5.2.2 事件紀錄查詢

5.2.2.1 測試方法

（1）登入待測物管理頁面。

（2）執行事件紀錄查詢功能。

5.2.2.2 合格標準

待測物應提供下列項目查詢功能，且可正常運作：

（1）事件發生日期及時間。

（2）事件觸發者。

（3）事件類別。

5.2.3 韌體檔案測試

5.2.3.1 測試方法

檢視經拆解韌體之系統檔案資訊。

5.2.3.2 合格標準

（1）系統檔案目錄不得檢出；或

（2）系統檔案不得檢出下列資訊：

A.未經加密之帳號密碼。

B.加解密用之金鑰（不含非對稱加密用公鑰）。

C. 韌體內第三方開源軟體元件未檢出 CVSS 嚴重性等級為高（High，即 7 分以上）之 CVE。

5.2.4 韌體版本更新測試

5.2.4.1 測試方法

（1）檢視待測物目前韌體版本。

（2）依照申請人提供的韌體更新方法執行韌體更新。

（3）中斷進行中的韌體更新程序。

（4）執行申請人宣告之回復韌體更新前狀態步驟。

（5）修改韌體數位簽章並重複步驟（2）。

（6）以完整韌體重複步驟（2）。

（7）以低於待測物目前韌體版本的韌體執行步驟（2）。

5.2.4.2 合格標準

（1）執行測試方法（2）後，待測物應產出相關紀錄。

（2）執行測試方法（4）後，待測物仍可回復韌體更新前之狀態。

（3）執行測試方法（5）後，待測測應無法完成韌體更新。

（4）執行測試方法（6）後，待測物韌體應為更新後的版本。

（5）執行測試方法（7）後，待測測應無法完成韌體更新。

5.2.5 預設密碼安全測試

5.2.5.1 測試方法

（1）檢查二待測物於原廠設定狀態下之管理者密碼是否相同。

（2）二待測物之預設密碼相同者，以管理者身份登入任一待測物。

5.2.5.2 合格標準

（1）二待測物於原廠設定狀態下之管理者密碼應相異；或

（2）首次以管理者身份登入待測物後，待測物應要求管理者變更密碼。經以變更後之密碼登入，始得使用管理者權限。

5.2.6 網路服務管控測試

5.2.6.1 測試方法

掃描待測物於原廠設定狀態下啟動之網路通訊埠。

5.2.6.2 合格標準

（1）啟動之網路通訊埠應符合申請人宣告之內容。

（2）不安全通訊埠（如 FTP、Telnet）應預設關閉。

（3）從遠端通訊埠登入至設備須符合 5.4 身分鑑別與授權機制安全規定。

5.2.7 作業系統與網路服務測試

5.2.7.1 測試方法

（1）更新測試設備系統脆弱性偵測功能之 CVE 脆弱性資料庫，該資料庫應包含 NIST 發布之 CVE，及採用 NIST 發布之脆弱性評估方式。

（2）掃描待測物通訊介面或管理頁面。

5.2.7.2 合格標準

待測物不得檢出 CVSS 嚴重性等級為高（High，即 7 分以上）之 CVE。

5.2.8 設備狀態回傳測試

5.2.8.1 測試方法

（1）中斷待測物與基地臺間之通訊鏈路。

（2）中斷待測物與用戶終端設備之通訊鏈路逾申請人宣告之時間。

5.2.8.2 合格標準

（1）待測物應提供簡訊或傳送異常訊息至特定 IP 之警示機制；或

（2）待測物正常運作時，固定傳送訊息，但異常行為時，不傳送訊息者。

5.3 通訊安全

5.3.1 無線通訊介面安全設置測試

5.3.1.1 測試方法

以無線網路分析工具分析待測物使用的加密連接模式。

5.3.1.2 合格標準

（1）待測物未提供無線接取管理頁面之功能；或

（2）待測物無線接取功能應預設關閉。

（3）待測物未使用公認不安全的加密連接模式。

5.3.2 通訊傳輸安全測試

5.3.2.1 測試方法

錄製封包並檢視封包內容。

5.3.2.2 合格標準

（1）安全通道應採用 TLS1.2 以上。

(2)傳輸資料須採用 AES 128 位元或同等加密強度之加密演算法。

5.4 身分鑑別與授權機制安全

5.4.1 鑑別及權限測試

5.4.1.1 測試方法

（1）輸入錯誤之帳號密碼登入待測物。

（2）以正確之管理者帳號與密碼登入待測物。

（3）執行該管理者所賦予權限可使用之功能。

（4）以不同權限之帳號與密碼登入待測物。

（5）執行該管理者所賦予權限可使用之功能。

5.4.1.2 合格標準

（1）輸入錯誤密碼時無法登入待測物。

（2）使用者帳號非常見帳號。

（3）輸入正確的帳號及密碼始可登入待測物，並具完整安全功能設定權限。

（4）帳號權限功能應符合其權限。

（5）區分管理與一般使用的兩種權限。

（6）無線連接與管理介面帳號密碼應分開設置且不相同。

5.4.2 連續鑑別登入失敗處理機制測試

5.4.2.1 測試方法

（1）使用一帳號並連續輸入 5 次錯誤之密碼登入待測物之管理頁面（若待測物因錯誤次數達設定上限而主動中斷連線者，不在此限）。

（2）待測物具帳戶鎖定功能者，經閒置超過帳戶鎖定設定時間後，再以同一帳號及正確密碼進行登入。

（3）使用另一帳號重複步驟（1）至（2）。

5.4.2.2 合格標準

（1）連續登入失敗後，在帳戶鎖定時限內應限制後續所有登入。

（2）所有帳號登入都應符合登入失敗處理機制。

5.4.3 登入畫面保密功能測試

5.4.3.1 測試方法

登入待測物。

5.4.3.2 合格標準

登入頁面應以特殊符號（如：＊）遮蔽輸入之明文密碼字元。

5.4.4 密碼複雜性測試

5.4.4.1 測試方法

變更管理者密碼，並以不同字元及長度組合設定之。

5.4.4.2 合格標準

（1）密碼應由英文大小寫、數字或特殊字元任意 3 種以上組合而成。

（2）密碼長度 8 個字元（含）以上。

5.4.5 操作逾時功能測試

5.4.5.1 測試方法

（1）設定待測物權限保護或管理者自動登出時間。

（2）登入待測物，並閒置超過權限保護或管理者自動登出之設定時間。

5.4.5.2 合格標準

（1）閒置超過權限保護或管理者自動登出設定時間後，待測物應自動顯示鎖定或重新登入畫面，且任何人無法讀取其管理畫面資訊或進行操作。

（2）待測物具自動鎖定功能者，經重新輸入正確密碼，始得登入使用。

（3）待測物具重新登入功能者，經重新輸入正確帳號及密碼，始得登入使用。

附表、設備概述說明

設 備 識 別		
設備名稱		
廠牌		
型號		
申請者 （公司、商號名稱）	□製造商 □進口商 □經銷商	
製造商		
軟、韌體版本		
使用之網路通訊埠 及個別用途		
設備資訊回傳管理端 之間隔時間		
範 圍		
實體範圍		
邏輯範圍		