第九次實驗室一致性會議

台北, 01/19/2021

會議紀錄

1 時間：2021 年 01 月 19 日下午 2:00-4:00

2 地點：TAICS 第一會議室

3 出席人員姓名(敬稱略)：

主席：陳曉強　　紀錄：廖文華

出席人員(敬稱略)：

經濟部工業局 林青嶔

中華電信股份有限公司中華電信研究院 羅盛楨

台灣德國萊因技術監護顧問股份有限公司 沈雨澤

安華聯網科技股份有限公司 楊采彤

行動檢測服務股份公司 譚仲良、方盈智

財團法人台灣商品檢測驗證中心 王煜詔

財團法人電信技術中心 吳勁僖

勤業眾信聯合會計師事務所 王晨芳

資誠聯合會計師事務所 李國樞

數聯資安股份有限公司 沈智揚、張皓勤

Bosch(台灣博世) 張偉倫、呂學儒

慧友電子股份有限公司 黃熙哲

財團法人工業技術研究院 卓傳育、趙翎廷

財團法人資訊工業策進會 高傳凱、秦燕君

台灣資通產業標準協會 周勝鄰(on line)、陳曉強、戴武聰(on line)、廖文華、辛坤瑩

4 提案討論

4.1 全盲(滲透性)測試導入網路攝影機資安驗證制度說明

4.1.1 為免除測試規範修訂作業之冗長與耗時，以加速全盲(滲透性)測試之導入，特邀集產、官、學專家依網路攝影機資安相關標準提供全盲(滲透性)測試導入之建議及可行性評估與方案。 經整合專家會議意見及會後意見之反饋，且基於時效之考量，確立於現行網路攝影機資安驗證制度所施行檢測項目，依可行性評估擇特定項目平行納入既有測試規範及全盲(滲透性)測試方法多重選項。經由此平行先導

作業，亦有助於全盲(滲透性)測試應用實務之累積以利後續相關測試規範改版作業。

4.1.2 綜合專家建議特定全盲(滲透性)測試選項制定適用項目一覽表，如附件一。

4.1.3 特定全盲(滲透性)測試項目之選用與測試案例(方法)之設計及其確效於進入實質檢測階段前須取得驗證機構(TAICS)之核可。申請選用特定全盲(滲透性)測試項目及其核可作業流程參見附件二。

4.1.4 產業標準重點在於產業，是經過產業重要關係人一起來制定，進而具意願共同遵循。 網路攝影機監控標準於 2017 年 5 月 5 號提案，歷經 7 個月 12 道程序(包含提案、草案修訂、廠商邀請、TMC 會議、理監事會審) ，一個非常嚴謹的過程，在 2018 年因應需求，展開第二版的修訂及公告。產業標準會因應技術持續的精進而步入標準修訂程序，然不會因應個別廠商的特殊狀況或需求而草率的更動既定的標準。往後若有相關 IP Cam 等相關標準的制定或修訂，協會將會透過公開及主動邀請的方式，希望大家能夠踴躍參與。

4.1.5 上項決議與作業流程，若無其他異議，將於 110 年 3 月上旬公告施行。

4.2 系列認證

4.2.1 系列產品的定義由申請者(及廠商)自行決定。

4.2.2 固定加測：網頁弱掃、系統弱掃；外觀或電路板上配置不同，亦須加測實體安全。

4.2.3 系列產品驗證所需測試項目，除上項規定外，由認可實驗室依系列產品與原登錄主產品差異點可能衍生資安風險與標準條文確認與執行。

4.3 能力比對試驗

4.3.1 時間預計定在第三季，對象為 IP CAM 認可實驗室，依比對採購數量採循環排程模式或同時寄件至所有實驗室執行之，參與費用待公告。

4.4 模糊測試

4.4.1 依 2020 年 1 月 9 日第六次驗證一次性會議決議，由於模糊測試工具的維護成本高，在資安測試市場未達到一定規模時難以支撐，故當次會議決議，接受委外測試，凡經 TAF 或 ILAC 認可的資安實驗室可委託執行。

4.4.2 未來 2、3 級實驗室若不具備 fuzzing 的測試能力，將會註明在 TAF 證書上，測試報告必須註明 fuzzing 相關測項不在 TAF 認可範圍。

4.5 測報之韌體版本資訊必須註明 hash 值。

4.6 Q&A

4.6.1 安華聯網：5.1.1.1 的實體介面安全管控測試 ，產品如果可以進入作業系統，廠商要給我一些工具去做測試，看有沒有符合身份驗證要求。那如果廠商沒有提供進入作業系統的時候，我們需要提出一些方法來驗證他沒有。也就是說客戶他今天給我一個產品是說，沒有提供進入作業系統的方法，是否代表他這一項是必要進入滲透測試的方案？

廠商：原來的這個規範，就是寫說廠商只要宣告有沒有 debug mode 的話，這個條款視同通過，原本條款是這樣寫的，那現在變成如果要做滲透測試，我們一定要提供這個 pin 腳出來，可是對我們來說，這個產品它是一個市售的產品，是完全沒有任何的這種 debug mode 的介面或是從外觀上來看，看不出任何的一個接腳，這是我們產品上的機制，這個測項對我們來講，我們認為這個就是沒有這個介面，仍要維持沒有介面。

結論：5.1.1.1 測試方式建議請廠商務必拉出 debug pin 以便測試人員確認是否存在可存取 OS 的實體介面(可採用邏輯分析儀或 JTAG Emulator 等)。若是文件說明無進入系統除錯模式之方法或無文件說明，則實驗室需提供相關嘗試測議之證明確無。測試時需依產品電路板而定，如無明顯接腳或接腳分散不易測試則無法進行。

4.6.2 工研院：5.2.2.1 是網路服務最小化的測試，驗證產品是否存在預期以外的網路埠跟 5.3.2.2 所講的網路介面存取設置測試是因為找不到，邏輯上會不會有些衝突？通過網路埠最小化測試的話，在 5.3.2.2 是否就能保證說它沒有額外的存取。

結論：5.2.2.1 跟 5.3.2.2 這兩個的針對的測項不一樣。5.2.2.1 原本即是盲測，若 5.2.2.1 掃出額外的網路埠，即代表此測項不符合要求。 5.3.2.2 則被歸類為「不適用」項目，其要求不會因是否做滲透測試而變更，亦即不管是採用標準方法還是滲透測試，都有符合此項要求。

4.6.3 安華聯網：5.2.3.1(a)若是廠商不提供韌體或是韌體加密，實驗室無法測試，該如何解決？

廠商(博世)：「我們那時候卡到的兩個最大的問題，第一個 debug mode，第二個是韌體的 dump，就是要提供那個解密的這一塊，這是我們問題比較大的兩塊」。

結論：請廠商提供韌體 dump 方法及介面，將韌體萃取出後執行逆向工程，若可還原出檔案系統格式，則查找敏感性資料是否存在；若無法還原出檔案系統格式，則採用 16 進位編輯器，檢視是否有可識別之敏感性資料。如果無法 dump，廠商應提供加密韌體檔，先嘗試對加密的韌體進行解密，再進行本項測試驗證。

5 結論

5.1.1 全盲(滲透性)測試導入網路攝影機資安驗證制度，2 月底前可提出相關建議，若無收到其他建議，將會於 3 月 15 日正式公告全盲(滲透性)測試申請作業辦法。〈詳見附件一、附件二〉

5.1.2 系列產品驗證所需測試項目，由認可實驗室依系列產品與原登錄主產品差異點可能衍生資安風險與標準條文確認與執行（固定加測項目：網頁弱掃、系統弱掃；外觀或電路板上配置不同，亦須加測實體安全）。於公告後立即施行。

5.1.3 能力比對試驗時間預計定第三季，相關作業及參與費用待公告。

5.1.4 模糊測試接受委外測試，凡經 TAF 或 ILAC 認可的資安實驗室可委託執行。

6 散會(16:10)