營維處系統科重點工作報告 (113/12/10)

目錄

[**壹、** **國內外市場動態：無** 2](#_Toc184398256)

[**貳、** **重大案件：無** 2](#_Toc184398257)

[**參、** **重點工作事項：** 2](#_Toc184398258)

[一、 「D-Link數據機存在重大漏洞」應變措施 2](#_Toc184398259)

[**肆、** **近期(三個月內)重要工作事項：** 3](#_Toc184398260)

1. **國內外市場動態：無**
2. **重大案件：無**
3. **重點工作事項：**
4. 「D-Link數據機存在重大漏洞」應變措施

緣由：

1. 2024/11/11 TWCERT CC網站揭露本公司所使用之Dlink HGW 6740C數據機存在資安漏洞。
2. 2024/11/28 ITHome報導 [已終止維護的D-Link數據機存在重大漏洞，近6萬臺設備曝險 | iThome](https://apc01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.ithome.com.tw%2Fnews%2F166245&data=05%7C02%7Chstccm%40cht.com.tw%7C2cb02c72b6344d1a8ddd08dd14f3fdc7%7C54eb9440cf0345fe835e61bd4ce515c8%7C0%7C0%7C638689760354265951%7CUnknown%7CTWFpbGZsb3d8eyJFbXB0eU1hcGkiOnRydWUsIlYiOiIwLjAuMDAwMCIsIlAiOiJXaW4zMiIsIkFOIjoiTWFpbCIsIldUIjoyfQ%3D%3D%7C0%7C%7C%7C&sdata=BtGRL7Y3%2FzFtH6KiopzjAfSleFMqW17XttY4AsdE%2FxQ%3D&reserved=0) 文中提到：這批漏洞的危險之處，在於中華電信提供許多個人用戶及政府機關這款數據機，上述漏洞的影響範圍相當廣泛，估計有超過6萬臺裝置曝露於遠端執行任意程式碼（RCE）的危險，而且，這些裝置大部分仍在運作。
3. 資安處與網分討論後已於11/28陳報林大總及資安長「D-Link 6740C 漏洞議題」應變處理措施，亦已向賈總、郭副總、羅副總同步資訊。
4. 應變措施說明：

緩解措施：透過關閉設備網頁、SSH 及 Telnet 等服務埠來修補漏洞，初步驗證顯示此方法有效。

重要客戶設備優先更換：針對使用 D-Link 6740C 的政府機關及重要客戶，已逐步與客戶協商確認設備更換時間，最遲將於明年1月底前完成。(更換過程中，需將 VDSL 改為 FTTH 供裝，或建設其他廠牌的 VDSL 局端設備，並需配合客戶時間進行施工)。

其餘設備將陸續完成更換。

辦理情形：

1. **截至12/5止，D-Link 6740C 漏洞處理進度摘要如下**：

緩解措施：總數約23.6萬部，已完成74,399部 (31.57%)。(預訂113/12/13前完成)。

總數為最新盤點數據(含Routing mode與Bridge mode，只有Routing mode 約6萬部受到影響)，因程式執行不好判斷，故同步關閉影響服務 telnet/ ssh/ web埠，客網處觀察TRIS障礙系統暫未發現異常障礙量。

12/9前是由固維處批次執行script對HGW關閉服務port，若未開機則會執行失敗，預期成功率>70%。12/9後由RINOS接手，每天定期polling scan尚未關閉的設備執行關閉服務port。

重要客戶設備優先更換：GSN總數2,841，預訂114/01/20前完成。

1. 除了政府部門，企業客戶發現報導後也陸續要求更換設備。
2. 架構處及客網處陸續請TRIS提供資料，方式是提供該受影響客戶電路清單，由TRIS查詢清單中所有的HGW型號，並標示是否為受影響型號，另再找出對應電路所屬營運處及客網中心，方便客網處安排更換設備：

10/22提供政府GSN設備資料4,490路(含[SA05]P-6101C)。

11/25提供第1次台水HiLINK案1,615路電路設備資料，客網處說提供給TRIS的母體資料有誤，需再重新盤點請TRIS擷取。

12/4提供第2次台水HiLINK案4,369路電路設備資料。

12/4再要求提供星巴克案資料\_未單獨提供。

1. 另一款7740C雖尚未被揭露，但相同供裝在DAS-3626 VDSL，一樣存在相同問題。
2. 12/5與架構處討論後，由TRIS擷取所有企業客戶電路(企1~企3)HGW屬於受影響4型號 ([SA05]P-6101C、[FV30]DSL-6740C(AP)、[FV35]6740C 2T2R(兩支天線(內建AP)有BAR CODE)、[FV36]DLINK-DSL-7740C) 電路清單112,894路，提供給架構處及客網處討論依重要程度安排更換設備，就不需每有企業客戶反映就請TRIS取1次資料。

後續作為：

1. 若非企業客戶(如GSN)，一樣由架構處或客網處提出需求，由TRIS擷取相關資訊。
2. **近期(三個月內)重要工作事項：**

|  |  |  |
| --- | --- | --- |
| 項次 | 工作事項 | 重要milestone |
| 1 | FORCE移轉GCP 進度 | 1. FORCE已於12/1移轉入GCP公雲。 2. 預計12/11 DB啟用「僅允許SSL連線」、DB CPU降core、AP調降資源。 3. DB CPU使用率偶有超過50%，於12/5曾達80%，一般在40%以下，12/11先降core觀察。 4. AP 1周內使用率約20%，偶有突波達80%，應該是有異常程式，預計12/11調降資源。 |
| 2 | POMIS 2.0開發建置 | 1. QoS 2.0資料來源已變更為pomis 2.0，預計5月份暫不考核，6/1起正式考核。 2. 已完成：   12/6完成114年維護日誌年度計畫表   1. 進行中：   8.11機房資訊整理作業(凱威)  5.3.2待辦量功能模組及久未登入Mail通知(祥恩)  3.2 NMOSS與財產設定作業、3.3NMOSS設備名稱對照表，初步完成(缺待辦量)，柯主任驗證中(博崴)  5.8 施工商聯絡資料表開發，以統編向工商開放平台取得其他的廠商資料，由開發人員驅動，每季更新。(怡華)  5.3.3 SMR放電最低電壓統計，規劃前端和折線圖(祥恩)  5.3.2 SMR負載介接PAMS資料已提供，PAMS 10/28確認資料OK，後續再繼續討論資料提供方式(怡華)  7.1.2-5G C-RAN用電管理設定作業(柏宇、怡華)  5.11.1NOC告警訊息統計，等待防火牆開通(POSS->POMIS)，進度90%(瑞貞)  5.11.6 GNOC通報模組(IOC) (瑞貞)  新增2.5.1關鍵字統計:發電機運轉加載(90%) (瑞貞)  7.1.3 5G C-RAN用電管理設定簽核流程規劃(柏宇)  iEN資料取得討論，介接方式討論中。  5.10.1 環保局每日用油申報作業需求分析(博崴)  準備8.7 手機APP查詢(柏宇)  備用油資訊由Argus定時每3分鐘向POMIS詢問，再由Argus提供給EIS。電力處劉股長會再整理需提供的必要欄位資訊提供raw data給Argus，準備API上架申請。  網分規劃待POMIS完成C-RAN 機房用電資料收集後(113/11/30)=>待討論  POMIS系統開發樓層用電統計功能(預計114/Q1開發完成) => 柯主任說可能不好算，待確認。  蓄電池內阻抗量測作業，113/7/11 柏宇email 回覆 綜企處 許佳豪，有與柯致平主任討論下列這一項目的時程，請更改成~~113Q4~~完成 => 這是舊MAIL，後來有跟佳豪更改時程至114Q3 |
| 3 | 透過查修哥裝機哥APP遠端開啟交接箱 | 1. 透過裝查APP進行遠端查詢、開啟交接箱。 2. 寬網所5/16已初步完成WEB UI介面，6/6已提供API，查修APP已於9/4完成開發並製作教學手冊提供給客網處，客網處已安排台北三客進行POC。 3. 裝機APP 11/1完成。 4. 5/9會議有再提出一些新需求。   (1).以裝機哥及查修哥APP工作單開啟箱門  (2).查詢所屬客網內箱門位置及使用紀錄  (3).無單開啟所屬客網內箱門功能(新)  (4).施工人員申請交接箱施工暫離(新)  (5).交接箱巡勘功能(新)  (6).其他管理者需求功能(新)  (7).推播功能  (8).其他後續須追加功能(新)  (9)具開啟交接箱角色新增以客網中心設定權限。 |
| 4 | 發送客戶簡訊改用簡訊特碼 | 1. 已洽詢個人家庭分公司/數位生活產品發展處/訊息及代收應用科 申請程序。 2. 目前有3種簡訊傳送客戶(測速紀錄，固定IP資訊、拆機收回設備) |
| 5 | 居家安防案 | 1. 新裝寬頻捆綁由客網攜帶設備安裝 2. 既有電路加裝可DIY由神腦取貨或神腦宅配 3. 宅配不卡聯單，DIY失敗，由CAS受理出新聯單。 4. IP CAM設備異常朝向主動品保處理，由資分開發的APP提供一鍵申告，後台維運系統主動偵測並即時APP推播異常訊息，即時通知客戶並於APP提供一鍵申告功能(消客產品想節省成本傾向由CAS處理完成，不請客網查修) 5. 方案已大致確定：既有電路，門市會於SPAS輸入領料人員，fORDER會帶BarCode及領料人員給SPRO轉給FORCE，規劃由FORCE直接進行扣料回報。 6. 上游新增所有設備DIY識別給TRIS及FORCE，BSPM新增API可查詢居家安防設備狀態，以便供客網於APP確認安裝情形。 7. FORCE自動回報流程機制已完成，但因目前TOPS及SPRO須提供的介面規格未定妥，尚缺少設備回報部份細節資訊。 8. 資分SO劉欣和(9/3)：    * 高階首長會議表示暫不硬壓上線時程(變數太多)。    * 重要關鍵時程：SO完成整測、SO員工封測、BO品質小組驗證、BO員工封測。    * 會根據封測結果，及第二次整測通過才會定版，再啟動通知廠商5000台。 9. 9/19線上流程驗證，FORCE設備回報功能測試失敗，修改進行中，10/16上版。 10. 9/30規劃科家豪請FORCE、CAS新增簡訊通知     * 在fORDER聯單產生後通知CAS發送簡訊外     * 在施工後，由FORCE通知CAS發送服務啟用通知簡訊，CAS於10/24上線，FORCE於10/16上線。 11. 11/19有開會討論員工封測前準備工作。 12. 最近 SO(TL智聯+資分智聯) 完成 整測試報告 交付 BO。BO 會先進行 品質抽測。目前BO還在做封測前置準備。 |
| 6 | OneWeb低軌衛星上網服務 | 1. SPRO、FORCE及TRIS間整合OneWeb上網服務之供裝施工派工及障礙派工等功能。 2. FORCE要讓廠商輸入IMEI, SN, IP, GPS等資訊，送TINOS，但初期(6月底前)TINOS沒辦法與One Web介接，所以還是要廠商去通知國維。 3. 目前設備只有一型KYMETA HAWK u8。 4. QA已有4路測試案例，FORCE流程OK。 5. PAMS已將IMEI、SN資料送給TRIS，驗證OK。 6. 國維處鄭凱文股長提供施工單所需資訊：   (1).查勘派工:查勘日期,派工單號,站點聯絡人資訊  (2).施工派工:派工日期,施工地址,派工單號,IP,站點聯絡人資訊   1. 分階段進行：第一階段只做到裝機、竣工歸檔；第二階段加上查勘及查修。 2. 查勘與施工都是同包商，需查勘派工的原因：要請廠商備料...要有時間,還有被安裝的單位要同意施作的時間。 3. 查勘與施工都要核點，但不是CEMIS。 4. 6/3 BSS/OSS開始於QA環境測試。 5. 6/11~6/21 BSS/OSS開始於線上環境測試。FORCE於6/24已收到測試單，國維處測試OK。 6. 預計第二階段進行的自動化開通流程，TINOS已備妥，FORCE與TINOS介接開發中。(因受理未開始，外部網站的回報開發先暫緩) 7. 廖文豪科長通知，依林大總指示:OneWeb相關用戶資料具有機敏性要求,各系統必須加強客戶資料保護(包含隱碼,查詢紀錄稽核軌跡等)。FORCE及TRIS需針對OneWeb用戶資料進行隱碼，查詢須送IAS。 |
| 7 | 強化HGW密碼管控機制 | 1. HGW收到登入請求時，將自行隨機產生一組具時效性之登入密碼，經加密流程後產生QR碼，之後由APP掃QR碼取得登入密碼。 2. 資安所4/3已提供私鑰解密API範例。 3. 查修哥APP於5/29已完成，架構處建一網站提供掃描QR Code，查修哥APP已驗證完成。 4. APP金鑰刪除機制：每日第一次開啟APP需重新下載，每日密碼不同。 5. 新提需求：需於系統儲存解碼紀錄。 6. 經固設處、寬網所、客網處努力溝通，Zyxel同意於7/29提供具QRCode認證功能之測試版韌體，7/29驗證失敗，需再進行討論。 7. 8/27廠商已提供新版韌體給客網，客網安裝完成後有通知我們持查修哥APP進行解碼驗證，結果已可正常解密，但非原定的6碼數字，廠商須再修改韌體。 8. 資安長定deadline 是 10月。 9. 11.寬網所提供給廠商的密碼原則  * 密碼格式：六個隨機數字 * 輸入機制： 三次錯誤(跳回登入頁面，鎖住3分鐘) * 輸入時效：限制5分鐘內完成密碼輸入 (超過時間跳回登入頁面)  1. 考量9/30前須完成全部測試，請研究院寬網所協助與 Zyxel溝通，新版韌體已於9/26測試完成。 2. 文豪已準備移植查修哥HGW OTP功能到裝機哥。 3. 尚在討論一個問題，廠商沒有APP如何進行測試。 |
| 8 | 支援「電桿及箱體設置位置盤查改善專案」 | 1. 開發「交接箱及電桿盤查及改善」查詢及回報功能。(10/16) 2. 開發「交接箱及電桿盤查及改善統計表」。 3. 預計113年底完成。 |
| 9 | 無線所Wi-Fi小精靈功能移轉至裝機哥APP | 1. 新增評鑑小精靈功能(測速/訊號量測/回報功能) 2. 新增竣工小精靈AP竣工圖片上傳及查詢功能 3. 11/14公眾Wi-Fi網路評鑑檢討會 4. 預計114/7完成，8月客網POC。 |
| 10 | 裝查APP導入採用電商隱碼機制 | 1. 開發查詢對應聯電API並上架(已完成) 2. 開發接收通聯記錄API並上架(已完成) 3. 裝機APP開發一鍵撥號功能(已完成) 4. 三區POC單位於8/8中午切換啟動。 5. 發現問題：8/13上版修正    * 施工單內容有部分聯絡電話未隱碼，需將施工單個資欄位進行清除。    * 裝機哥簡訊(測速結果簡訊、拆回設備證明簡訊、客戶固定IP資料)未考慮聯絡電話已隱碼，導致無法發送，需後端解碼後再發送。 6. 客網線維中心請POC單位於9/5前提供試用發現問題，於9/11開會檢討。 7. 客網裝機APP隱碼功能POC，預計9/25 12:00擴大整個新北營運處試辦，由先前的1個客網(新北一)增加至4個客網中心。 8. 客網處志豪：針對撥出縮短時間部分，客網處請行設處將”轉接中..請稍後”5秒時間取消掉。行動通信規劃設計處通知9/25已完成音檔置換。 9. 放心接新增顯示分機及電話後3碼功能，9/25上版。 10. 第二階段POC作業:規劃擴大至新北、台中、高雄三個營運處自10/16至12月底辦理，並計畫於114/01/01 起推廣全區使用。 11. 11/11變更語音檔內容： 12. 針對隱碼作業提供裝機前簡訊通知及聯繫不到客戶發送罐頭簡訊(預計12月底完成)     * 施工前簡訊內容標示代表號，讓客戶安心。     * 聯繫不到客戶，透過裝機哥發送簡訊給客戶。 |
| 11 | 支援全面擴大客戶查修竣後雙向關懷簡訊作業 | 1. TRIS系統判斷「非VIP客戶障礙申告案件」修復(ABC項正常結案)時篩選行動聯絡電話，傳送至CAS系統發送修復關懷雙向簡訊給客戶。 2. 停止原單向修復關懷簡訊。(8月底) 3. 客服處郭股長需求，現行VIP客戶障礙修復雙向關懷簡訊由原限制(HiNet 300M(含)以上)擴大至全部VIP客戶適用，6/26上版。 4. 7/31寬頻優化會議，個家張協理追蹤此案進度，經與個家客服處、CAS協調於9月底上版。 5. 9/23客服通知，CAS非VIP客戶查修竣後確認/關懷作業上線日期為9/26。由宏華三部承接，請CAS派案至2-7中心一股。原TRIS非VIP客戶查修竣後確認/關懷作業上線日期為10/16。客服再次通知因颱風因素，座席量能不足，請TRIS延後上版，預計延至11月。 |
| 12 | 資訊系統入公雲之成效查核專案\_改善追蹤(TRIS內稽待改善事項相同) | 1. 資料庫僅允許SSL加密通道，程式已修改上版完成，5/28中午12:10 DB啟用僅允許SSL連線。 2. 資料庫個資欄位加密：    * 階段一：個資數量較大但較易處理部份預計於113/8/31前完成。    * 階段二：較複雜影響較大部份，預計於113/12/31前完成。 3. 執行進度：    * 6/19先新增1個資Table，含4個資欄位(申告聯絡人、電話、MAIL、行動號碼)，進行測試。    * 加解密共用元件已開發完成。    * 申告介面程式修改進行中，新舊Table同步寫入，資料加密後再寫進新table。    * 已完成申告聯絡資訊的加解密開發，6/28已於QA測試完成，未發現問題。    * 目前盤點出9個Table需處理    * 客服有以聯電向TRIS模糊比對查找障礙電路資訊功能，加密後會無法比對，改以hash方式處理，11/27上版。 |
| 13 | 會計師外稽資料準備 | 1. 系統需準備佐證資料16~88項，已於6/21上傳完成。 2. 7/2 14:00進行初步訪談。 3. 12/12進行FORCE外稽訪談。 |
| 14 | EAI 服務移轉APIM啟動會議 | 1. 7/23 10:00資分數位中台針對EAI平台上的所有後端系統召開會議，會議說明服務移轉至APIM的相關資訊。 2. 目標：114/4月前於EAI上架的服務一率改上架至APIM2.0。 3. 盤點FORCE尚有4項服務需移轉。 |
| 15 | 支援客網伴銷話機 | 1. 查修哥APP新增行動支付功能。 2. 11/4已提供查修哥線上APK檔給彰化營運處進行線上POC，預計本週會完成測試。 3. 行動支付目前限定要有載具，銷退一律請客戶帶設備至門市辦理。 4. 11/14 客網伴銷話機-受理系統第二次討論會議，開始進行列帳功能討論。 5. 截至11/25 彰化2個客網的宏華隊長共測試5筆    * 1筆送POS失敗：POS API修改變更URL，查修哥配合更新完成。(11/19)    * 2筆測試誤刷支付條碼情境失敗，查修哥APP要修改POS回應支付失敗時要允許能重複刷支付條碼。 6. 時程：    * 彰化POC預定於113/11月底完成。    * 其他營運處預定，由全省各客網宏華查修指派種子人員進行POC，預計12月底完成。    * 全區上線時程因牽涉金流、物流兩部分，需嚴謹無問題才會正式上線，預計時程排在114/1月。 7. 11月底彰化服務中心反應帳有問題，引起帳務處理困擾，先暫停測試，今日詢問POS已修復，可再繼續由彰化營運處繼續測試。 |
| 16 | FORCE提供speedtest統計報表 | 1. 10/30完成月報。 2. 後續開發日報功能。 |
| 17 | 113年下半年開源軟體檢測 | 1. 待修補  |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | FORCE\_OL | FORCE\_QA | TRIS\_OL | TRIS\_QA | | 10/22 | 50 | 4 | 1 | 0 | | 11/11 | 16 | 1 | 0 | 0 | | 11/18 | 15 | 1 | 0 | 0 | | 12/10 | 0 | 0 | 0 | 0 | |
| 18 | 查修哥APP新增MOD查測功能 | 1. 因「宜蘭部分MOD用戶無法觀看VoD及Netflix障礙討論會議」會議紀錄，查修哥APP介接BSPM，新增MOD查測功能。 2. BSPM ping CDN IP功能，BSPM 已提供網頁版本，於12/4已將API提供給查修哥開發，查修哥預計12/25上版。 |
| 19 | 個家客服處再OT資訊系統應變 | 1. TRIS及FORCE有介接LDAP人員異動資料，當日排程暫停執行，由人工確認檔案標誌後再執行。 2. TRIS含有客服單位代碼，需有對照表參考後當日更新。 |