110年第3季資通安全技術報告

Quarterly Technical Report

目　次

1. 資安威脅現況與防護重點 3
1.1 全球資安威脅現況 3
1.2 政府資安威脅現況 4
1.3 資安防護重點 7
2. 資安專題分享_ OWASP Dependency-Track 元件分析平台 9
2.1 Dependency-Track 概述 9
2.2 Dependency-Track 實作驗證 10
3.資安技術研析_WaterBear 攻擊分析 14
3.1 WaterBear 新型態樣本分析 14
3.2 中繼站追蹤分析 16
4. 結論 18
資安相關活動 19
110 第 1 次政府資通安全防護巡迴研討會 19
N-ISAC 會員會議 19

圖 目 次

圖 1　110 年第 3 季通報事件影響等級比率圖 5
圖 2　110 年第 3 季通報類型比率圖 6
圖 3　110 年第 3 季公務機關資安事件原因比率圖 7
圖 4　Dependency-Track 平台 10
圖 5　新增 CycloneDX 外掛 11
圖 6　簽入含有不安全元件(httpclient 4.5.10)之測試專案 12
圖 7　Dependency-Track 平台弱點檢視與郵件通知 12
圖 8　弱點修補後驗證顯示結果 13
圖 9　WaterBear 樣本行為鏈 15
圖 10　測試樣本加密資料顯示 16
圖 11　利用漏洞獲取帳密 16
圖 12　受駭單位類型統計 17

摘要

「第 3 季資通安全技術報告」除分析本季全球資安威脅、政府通報資安事件外，並提供相對應之資安防護建議。同時，藉由資安專題分享與資安技術研析，提供政府機關最新資安風險之關注重點。

「第 3 季資通安全技術報告」分為以下 4 個章節。

●1.資安威脅現況與防護重點

從分析全球資安威脅現況開始，第 1 起案例為以色列軍事級間諜程式 Pegasus 遭濫用於監控全球政要與記者手機；另一起案例為印尼防疫資料庫未妥善進行防護，導致上百萬人資料外洩。

分析政府資安威脅現況，發現政府機關通報事件，以「非法入侵」(占 68.08%)類型為主，排除綜合類型「其他」外，其次分別為「網頁攻擊」(占 6.1%)」與「設備問題(占 5.16%)」為主要通報類型。

●2.資安專題分享

資安專題分享主題為 OWASP Dependency-Track，概述可用於開發過程中盤點系統元件之工具，並檢測是否具有已知漏洞，可強化安全系統發展生命週期(SSDLC)於開發階段之安全性。

●3.資安技術研析

資安技術研析主題為 WaterBear 攻擊分析，近期分析攻擊型態樣本發現該惡意程式為 WaterBear 後門程式。針對中繼站進行追蹤分析，並分析 WaterBear 新型態樣本，了解其攻擊模式。

●4.結論

本報告透過分析全球與政府之資安事件與統計數據，了解最新資安威脅趨

勢與因應之資安防護重點。資安專題分享 OWASP Dependency-Track，用於開發過程中盤點系統元件，並檢測是否具有已知漏洞。此外，資安技術研析主題為 WaterBear 攻擊分析，分析攻擊型態樣本發現該惡意程式為 WaterBear 後門程式。針對該惡意中繼站進行追蹤分析，了解其鎖定對象、入侵路徑及相關攻擊手法。

1. 資安威脅現況與防護重點

本報告藉由檢視當季國內外所發生之資安事件或議題，研析事件發生之主要原因及可能之衝擊與影響。110 年第 3 季(以下簡稱本季)探討軟體供應鏈風險與如何加強資通系統防護，以避免遭受攻擊致資料外洩。

本章節之事件與議題皆配合整理相關之資安防護重點，提供政府機關就相關資安風險或議題進行評估，並依循資安管理規範與技術防禦進行強化。

1.1 全球資安威脅現況

隨著科技發展，許多資通訊技術之發展，初始時立意良好，但猶如雙面刃般，一但被不法人士所利用，則原本用為協助追蹤入侵者之利器瞬間轉為駭客武器。最佳演繹案例為以色列間諜軟體領導品牌公司所開發之程式遭濫用，該軟體起初以網路釣魚方式，寄送惡意連結後，使用者需點擊才會中惡意程式。但因該軟體現已進化至無需點擊即可從遠端安裝後直接控制手機，思考該軟體被若惡意人士濫用，後果將不堪設想。此特殊技術運用案例，提醒資安防護人員除應關注已知之風險外，亦應研究最新攻防技術，預作防範準備。

本季具指標性案例為以色列軍事級間諜程式 Pegasus 遭濫用於監控全球政要與記者手機；另一起案例為印尼防疫資料庫未妥善進行防護，導致上百萬人資料外洩。

首先，探討案例為以色列軍事級間諜程式 Pegasus 遭濫用事件，Pegasus 由以色列網路情報公司 NSO Group 開發，銷售予各國軍方、執法部門及情報部門，用於協助追緝可能透過加密通訊軟體逃逸之犯罪者，具有多元入侵手機之技術，如透過釣魚網址與彈出式廣告等方式誘使使用者造訪惡意網站，或無需透過手機持有人執行任何動作之零點擊(Zero Click)攻擊方式，即可將間諜程式 Pegasus 安裝於 Android 或 iPhone 手機上，該程式不僅可 24 小時監控手機，同時能將用戶個人資料、訊息、照片及通話等資料傳送至遠端

伺服器，亦可遠端啟動手機麥克風與相機，記錄受駭者通話內容。

事件起因為國際特赦組織收到疑似遭到 Pegasus 監控之 5 萬筆電話號碼資料庫，藉由非營利組織禁忌故事(Forbidden Stories)協調下，與國際媒體合作進行調查，實際取得且分析多支手機發現，部分已遭成功植入間諜程式 Pegasus，另有其他手機存在遭嘗試入侵之跡證。

第 2 起案例為印尼防疫追蹤 APP 使用之資料庫未妥善進行防護，導致約 130 萬人之 COVID-19 檢測資訊、醫療紀錄及個資等機敏資訊外洩。研究機構 vpnMentor 發現，印尼防疫追蹤 APP eHAC(eHealth Alert Card)使用之 Elasticsearch 資料庫配置錯誤，導致資料外洩事件。eHAC 為印尼政府開發之防疫追蹤 APP，要求所有入境印尼與搭乘國內班機之國內外旅客登錄資料，內容包含個人姓名、身分證號碼、COVID-19 病毒篩檢結果、住處及其他個人醫療相關資訊等。

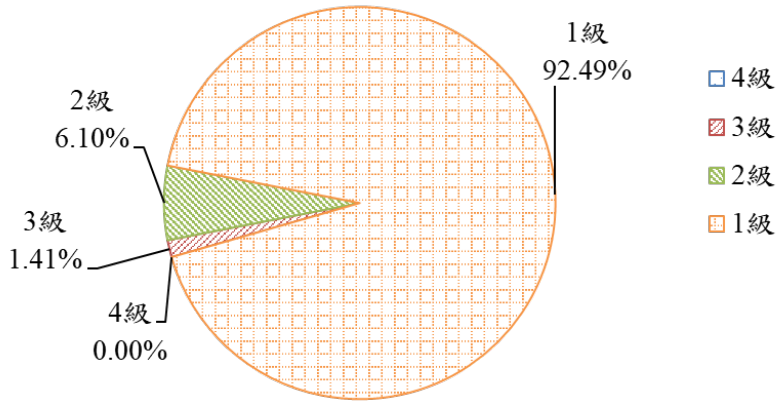
vpnMentor 於 7 月 15 日發現曝光之資料庫，並於 7 月下旬分別通知印尼衛生部、國家 CERT 及代管服務提供者 Google，歷經 1 個月後才得到印尼政府回應，說明自 7 月起不再使用 eHAC。

綜覽本季重大資安事件，資通訊技術不論是間諜程式或資安攻防程式遭濫用，已是可見之未來趨勢。因此，如何在進行科技發展同時，兼顧合法應用與避免濫用，當是開發人員首要之責。同時，在新冠疫情除造成社會經濟受影響外，因疫情所衍生出之資訊蒐集與應用，更需考量處理、利用、儲存，甚至後續刪除等管理責任。

1.2 政府資安威脅現況

彙整本季所接獲之政府機關通報事件，藉由事件之影響等級、通報類型及事件原因，了解目前政府機關之資安威脅現況。通報事件依「機密性」、「完整性」、「可用性」等 3 個面向所造成之衝擊，將事件影響等級由輕至重分

為 1 級、2 級、3 級及 4 級。彙整事件影響等級，本季以 1 級事件占 92.49%為大宗，2 級事件占 6.1%次之，3 級事件僅占 1.41%，而 4 級通報事件則未發生，相關統計情形詳見圖 1。



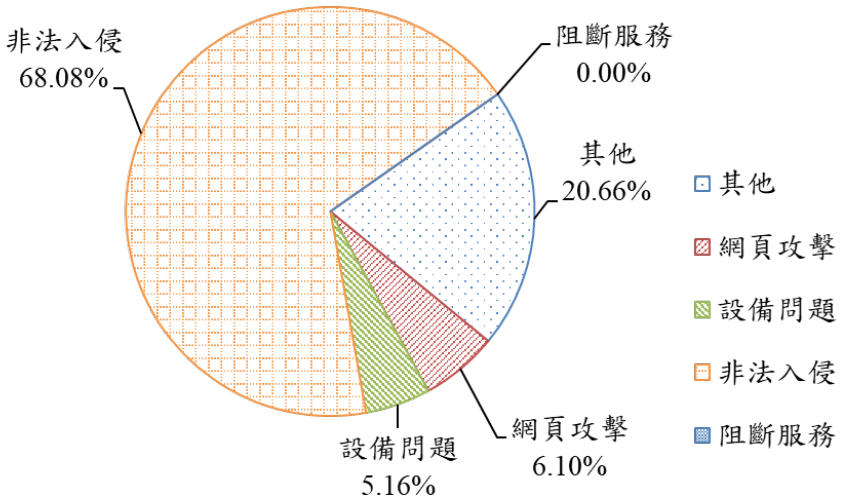
資料來源：本報告整理

圖1　110 年第 3 季通報事件影響等級比率圖

本季接獲之 3 級重要通報事件，以個人資料外洩事件居多，包含因 google 表單權限設定錯誤，致報名參加該場會議之個人資料可於網路上公開瀏覽。另一起案例為實兵演練所揭露之風險，發現機關提供予業者申請標章之系統具有無效之存取控制漏洞，若遭駭客成功攻擊，將可取得業者之身分證、手機號碼及電子郵件等個人資料。

除上述資安事件外，技服中心偵測發現數個機關有向挖礦報到連線行為，故發布警訊通知機關應變處理，部分機關調查發現安裝之 oCam 免費螢幕錄影軟體內嵌挖礦程式，導致機關對外連線礦池，部分機關則尚無法確認連線原因。

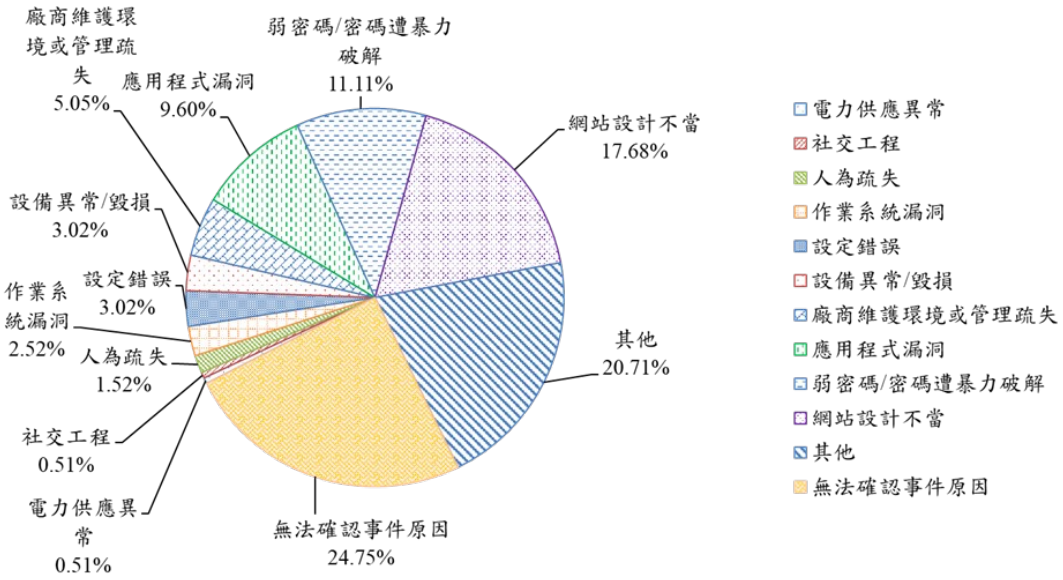
統計本季通報事件類型，以「非法入侵」(占 68.08%)類型為主，排除綜合類型「其他」外，「網頁攻擊」與「設備問題」類型次之，詳見圖 2。



資料來源：本報告整理

圖2　110 年第 3 季通報類型比率圖

進一步分析通報事件發生之原因(詳見圖 3)，可確認之事件原因分別為網站設計不當(17.68%)、弱密碼(11.11%)、應用程式漏洞(9.6%)、廠商維護環境或管理疏失(5.05%)、設備異常/毀損(3.02%)、設定錯誤(3.02%)、作業系統漏洞(2.52%)、人為疏失(1.52%)、電力供應異常(0.51%)及社交工程(0.51%)。統計本季事件發生原因，發現網站設計不當事件增加，如機關網站因業務需求必須開放民眾上傳檔案之功能，卻未限制上傳之檔案類型；另或因管理網站內容需要，於管理後台提供上傳編輯功能，疏於確實檢查上傳之檔案格式，相關網站功能之疏失設計與設定，可輕易遭駭客利用上傳惡意程式，進而展開進階或橫向擴散攻擊。



資料來源：本計畫整理

圖3　110 年第 3 季公務機關資安事件原因比率圖

1.3 資安防護重點

分析本季全球資安威脅現況，以色列間諜軟體所引起之恐慌在於不需點擊即可從遠端安裝後直接控制手機。此特殊技術運用案例，提醒資安防護議題已成為全民顯學，因為無法確切得知何時會成為受駭目標，更應時時關注所運用之資通訊設備安全，提升自身資安防護意識，強化防禦韌性與能力。

近來 APP 行動運用程式與網站設計不當等漏洞，屢屢造成駭客入侵或個人資料外洩等事件。隨著 APP 與網站設計需求之提升，系統開發專案強制要求資安規格與設計之載入已刻不容緩。另外，國內發生使用免費螢幕錄影軟體，卻內嵌挖礦惡意程式，亦暴露在使用共享或免費軟體時，可能因使用者或系統管理者之輕忽，未能提報或注意軟體之使用，而引起更大之資安風險。

綜整以上資安威脅現況，提供資安防護建議如下：

●共享或免費軟體之資安管理

– 建立內部已開放使用之共享與免體軟體清冊，包含版權宣告、版本及使用範圍等資訊。

– 定期檢視已下載使用之共享與免體軟體之系統安全性訊息，更新相關系統漏洞。

– 納入內部資通系統檢查項目，檢視安裝之必要性，若不再使用應儘速解除安裝。

●網站設計之資安管理

– 系統上線前應執行組態安全性設定與審查，訂定安全性檢核項目，並確認其符合性。

– 利用檔案檢測管理工具限制可儲存檔案格式與類型，並設定經允許之檔案執行功能。

– 檔案重新命名或設定僅允許唯讀模式，避免外部直接存取或執行檔案。

2. 資安專題分享_OWASP Dependency-Track 元件分析平台

OWASP Top 10: 2017 之 A9 指出，使用具有已知漏洞之元件(Using Components with Known Vulnerabilities)為資通系統常見之資安弱點。開發團隊通常高度使用開源軟體或元件進行開發，可能無法逐一了解應用程式或 API 中使用哪些元件，更遑論確認這些元件是否進行更新。因此，檢視資通系統所使用元件之安全性，不論是在程式開發或線上正式使用時，皆為重要資安課題。

為避免上述問題，OWASP Dependency-Track 專案提出一套第三方元件管理工具，此工具可用於開發過程中盤點系統元件，並檢測是否具有已知漏洞，可強化安全系統發展生命週期(Secure System Development Lifecycle, SSDLC)於開發階段之安全性。以下將針對 Dependency-Track 元件分析平台進行簡介，並進行概念性驗證。

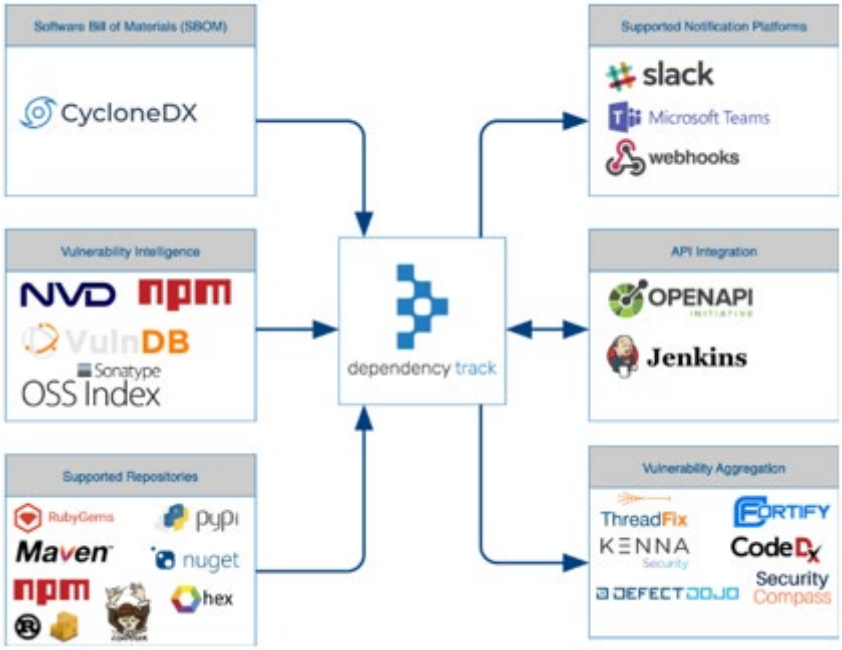
2.1 Dependency-Track 概述

Dependency-Track 為 OWASP 之旗艦專案(Flagship Project)，目前最新版本為 v4.3，因其具容易下載、安裝運作等特色，可減少部署與熟悉新開發工具時間，主要運用於開發元件分析平台(Component Analysis Platform)，分析元件之版本與弱點，並可整合於開發流程中，協助組織識別與降低軟體供應鏈中之風險。

Dependency-Track 提供多項特性與功能，且支援多種語言程式庫，如 Maven(Java)與 NuGet(.NET)等，提供之主要功能包含匯入元件清單功能，利用軟體物料清單(Software Bill of Materials, SBOM)之標準格式匯入，SBOM 為軟體所使用之元件列表清單，其中包含元件之標識資訊，如名稱、版本及授權方式等。SBOM 目前有多種標準格式，如 SPDX、SWID 及 CycloneDX 等。Dependency-Track 所支援之格式為 CycloneDX，其為輕量級 SBOM 標

準，支援多種開發工具產生 CycloneDX，如 CycloneDX CLI、CycloneDX .NET、CycloneDX for Maven 及 CycloneDX for Gradle 等。

Dependency-Track 藉由比對已知弱點，搜尋元件是否存在於弱點資料庫(如 National Vulnerability Database, NVD 等)，並採用 API 設計，適合在整合與持續交付(Continuous Integration, CI/Continuous Delivery, CD)環境中使用，運用 API 與 CI 工具，如 Jenkins 等串接至開發流程，詳見圖 4。



資料來源：本報告整理

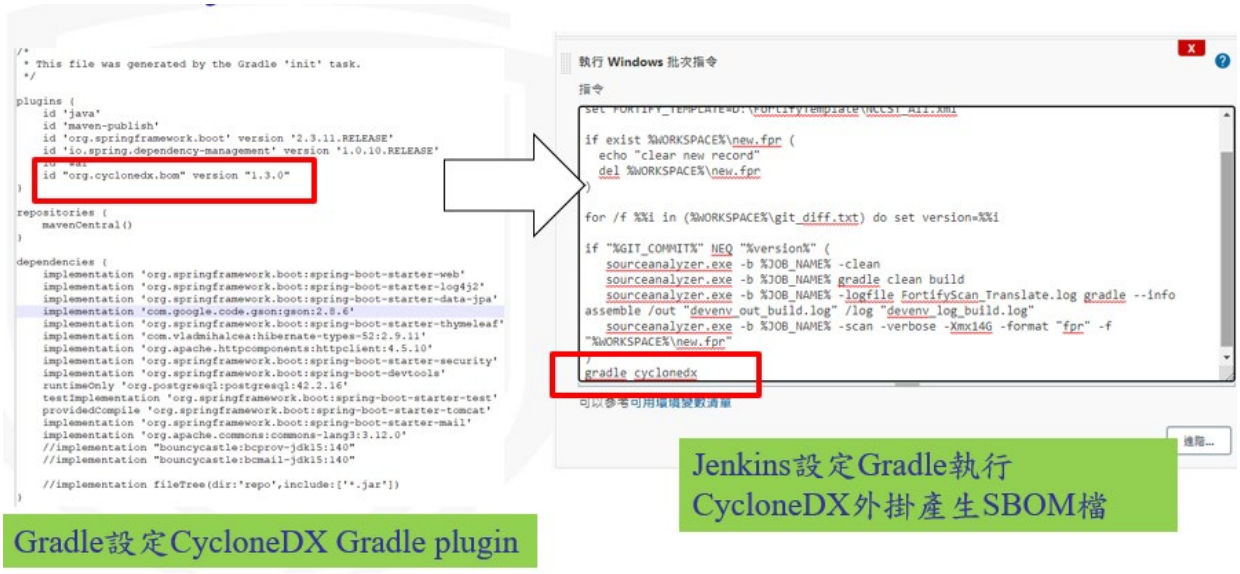
圖4　Dependency-Track 平台

俟 Dependency-Track 完成掃描檢測之後，即可於管理介面上檢視掃描結果，且亦可透過 Email 或即時通訊發送掃描結果通知，以下將說明 Dependency-Track 之概念性驗證程序與結果。

2.2 Dependency-Track 實作驗證

實作目的主要在驗證於開發流程中導入元件漏洞分析功能，並確認其可行性。首要步驟為架設 Dependency-Track 平台，並建立元件分析專案。每個

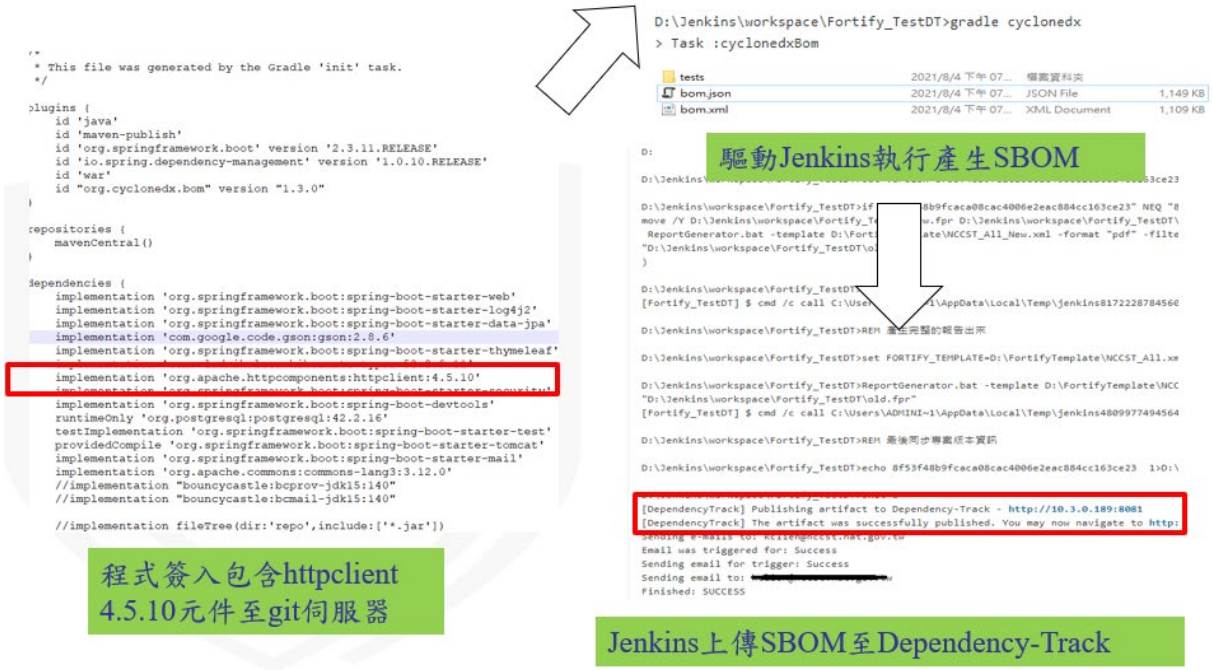
程式碼專案必須藉由建立相對應之元件分析專案，程式碼專案簽入至 Git 程式儲存庫，並觸發 Jenkins 啟動 CI 流程。接續於 Dependency-Track 平台設定團隊成員、上傳 API 權限及報告通知方式與條件。第三步驟利用 Jenkins 安裝 OWASP Dependency-Track Plugin，並設定上傳位置與 API KEY。第四步驟為編譯專案確認程式碼可正確編譯，於編譯工具 Gradle 中新增 CycloneDX 外掛，並設定 Jenkins 於每次呼叫 Gradle 編譯時一併產製 bom.json，詳見圖 5。



資料來源：本報告整理

圖5　新增 CycloneDX 外掛

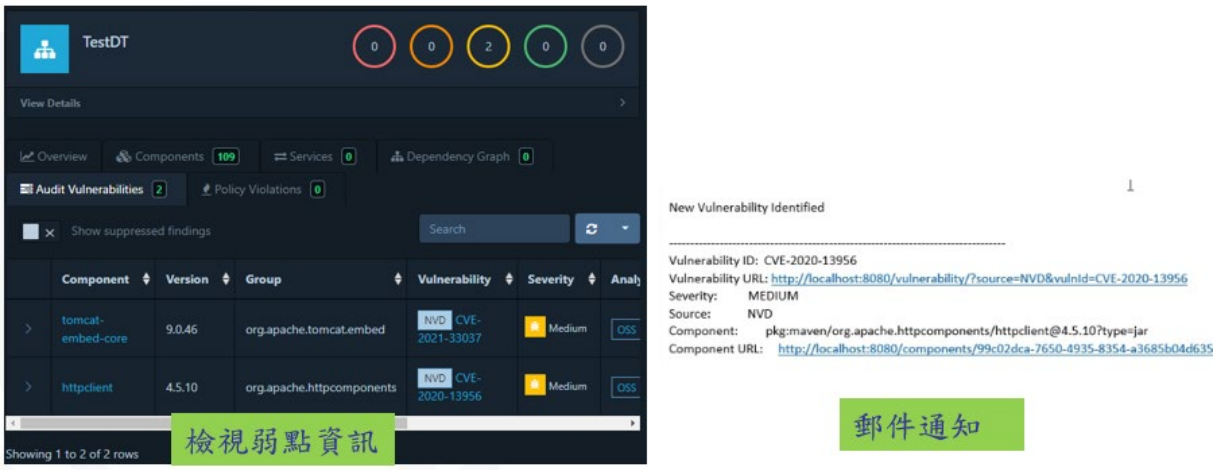
產製 SBOM 檔後，第五步驟於 Jenkins 新增工作任務，上傳 SBOM 檔至 Dependency-Track 平台進行元件漏洞分析。最後進行測試驗證實作，藉由簽入含有不安全元件(httpclient 4.5.10)之測試專案，測試其分析結果，詳見圖 6。



資料來源：本報告整理

圖6　簽入含有不安全元件(httpclient 4.5.10)之測試專案

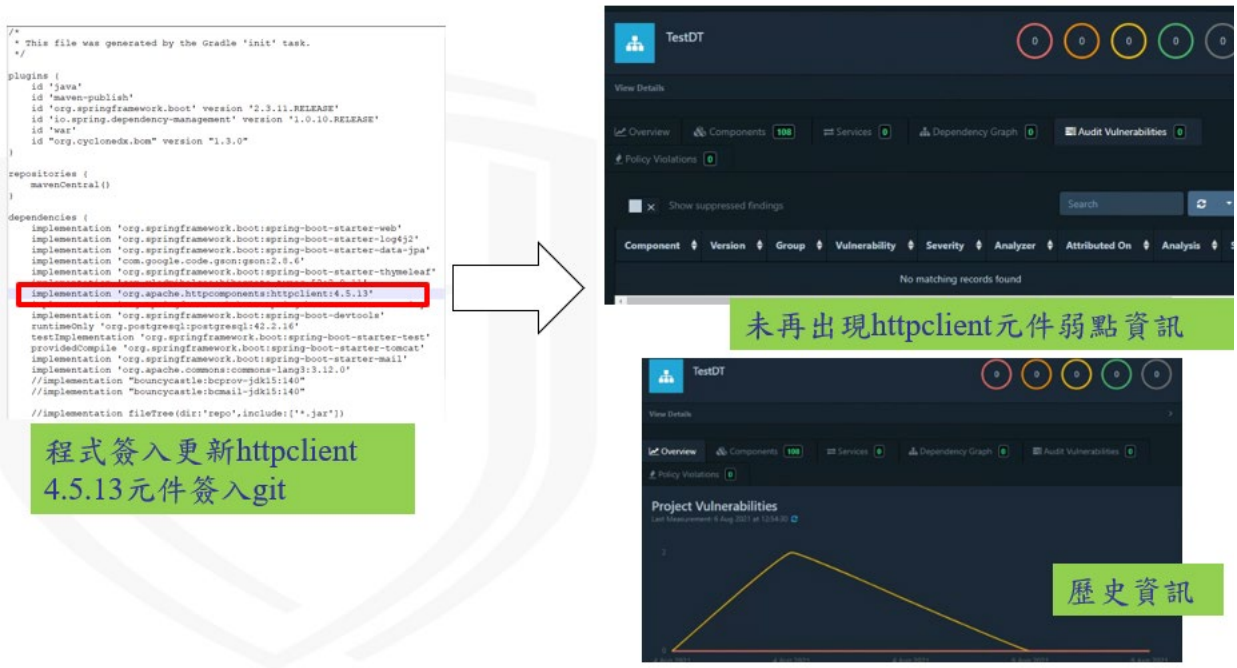
檢視 Dependency-Track 元件分析資訊與所收到 Email 通知，皆顯示該專案具有 CVE 漏洞，詳見圖 7。



資料來源：本報告整理

圖7　Dependency-Track 平台弱點檢視與郵件通知

依測試結果進行程式碼調修，更新元件後再次簽入程式碼專案，顯示已無元件漏洞。隨著系統開發專案過程，可藉由比對歷史資訊，檢視與追蹤漏洞修補情況，詳見圖 8。



資料來源：本報告整理

圖8　弱點修補後驗證顯示結果

SSDLC 之重要概念為基於安全設計(Security by Design)，設想系統開發過程對於所發現之系統漏洞或惡意行為進行防範，可能之風險情境包含第三方之元件。Dependency-Track 為免費開源之元件分析平台，可輕易整合至開發流程，因此技服中心藉由實作驗證測試其有效性，後續將陸續於內部開發環境中試行導入，以強化 SSDLC 開發階段之安全性，並將相關資訊運用推廣至政府機關。

3.資安技術研析_WaterBear 攻擊分析

本季探討之資安技術研析為 WaterBear 攻擊分析，國際資安組織觀察到有關 WaterBear 惡意程式之駭侵活動，並透過 TWCERT 發送情資示警。情資指出，110 年 3 月起發現該惡意程式攻擊我國政府機關與資通服務供應商，所幸相關中繼站均已事前掌握，並部署於政府網際服務網(GSN)骨幹網路進行偵測。

從 101 年 WaterBear 惡意程式開始在東南亞發動駭侵行動，鎖定日本、香港及台灣等進行 APT 攻擊，以竊取機敏資料。此惡意程式通常先鎖定目標對象是否使用存在 CVE 漏洞之路由器設備，再利用未即時更新或修改預設設定之設備展開攻擊，進一步取得該路由器控制權後，展開橫向入侵與攻擊活動。鎖定對象除政府機關與民間企業外，亦包含政府機關之資通服務供應商，藉由入侵其資通系統後，做為跳板再成功滲透政府機關。

以下將針對 WaterBear 新型態樣本與所使用之中繼站進行分析。

3.1 WaterBear 新型態樣本分析

110 年上半年發現大量 WaterBear 相關中繼站，經查共發現 66 個中繼站網域名稱(DN)，分屬 15 個網域，駭客大量註冊網域名稱，並視需求更新啟用。近期 WaterBear 樣本整體運作模式與以往樣本相同，僅在 shellcode 自身加密與載入方式有所變化，樣本行為鏈(behavior chain)詳見圖 9。

資料來源：本報告整理

圖9　WaterBear 樣本行為鏈

先前樣本多以成對出現(Loader+shellcode)，shellcode 通常為獨立檔案，由 Loader 啟動後讀取執行，近期樣本 shellcode 則會先經過加密再寫入登錄檔(registry)中，Loader 在啟動後讀取特定登錄檔欄位解密執行，整體運作模式與以往樣本相同，僅在 shellcode 自身加密與載入方式有所變化。

Shellcode 加密後會放在登錄檔之指定路徑中，儲存方式為 16 進位 hex 值。解密時則需呼叫 CryptUnprotectData API，並利用受駭電腦之 Master Key 做為解密金鑰使用，Master Key 通常用來加密保護系統中之憑證(Credentials)與 Cookies。為取得 Master Key，可利用 mimikatz 內建功能，分析所擷取 Windows 登入程序 lsass.exe 之記憶體內容，從中找到屬於該使用者之 Master Key。接續將 shellcode 密文存為二進位檔案，並利用 mimikatz 之 DPAPI 解密功能搭配 Master Key，即可解出 shellcode 明文內容。於實驗環境中，成功解密測試樣本之加密字串"test123123123"，詳見圖 10。

```
mimikatz # dpapi::blob /in:crypt.bin /masterkey:f1cd9063430dff9f52a1096b8a18fdc616ac29e2299e5437e
**BLOB**
  dwVersion          : 00000001 - 1
  guidProvider       : {df9d8cd0-1501-11d1-8c7a-00c04fc297eb}
  dwMasterKeyVersion : 00000001 - 1
  guidMasterKey      : {7ed8bee6-f1e7-46bd-a641-18de2aa7e34c}

 * volatile cache: GUID:{7ed8bee6-f1e7-46bd-a641-18de2aa7e34c};KeyHash:846a33012cc29011bcabb31785
 * masterkey     : f1cd9063430dff9f52a1096b8a18fdc616ac29e2299e5437ebbc73887f8dcdccd258e54b664dd0
description :
data: test123123123
```

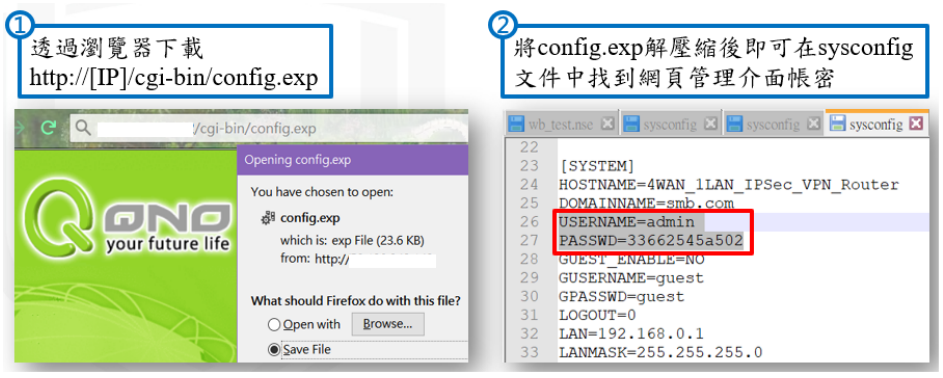
資料來源：本報告整理

圖10 測試樣本加密資料顯示

3.2 中繼站追蹤分析

針對近期 WaterBear 活動之中繼站進行調查，發現駭客依舊利用路由器之 VPN 功能做為跳板之攻擊模式。根據中繼站側錄之封包進行分析，發現連線報到受駭者不限於政府機關，所使用之網通設備皆為 QNO(俠諾)網通設備(QVF8027)。QNO 雖然未揭露任何公開之 CVE 漏洞，但分析多個設備型號韌體後，發現其韌體與 Cisco RVxxx 系列產品相似，存在共通弱點 CVE-2019-1653，導致駭客可利用韌體公開弱點入侵。

CVE-2019-1653 漏洞為身分鑑別之漏洞，遠端攻擊者不需登入即可利用此漏洞取得該路由器之設定，包含網頁管理介面帳密與設備配置細節等，詳見圖 11。

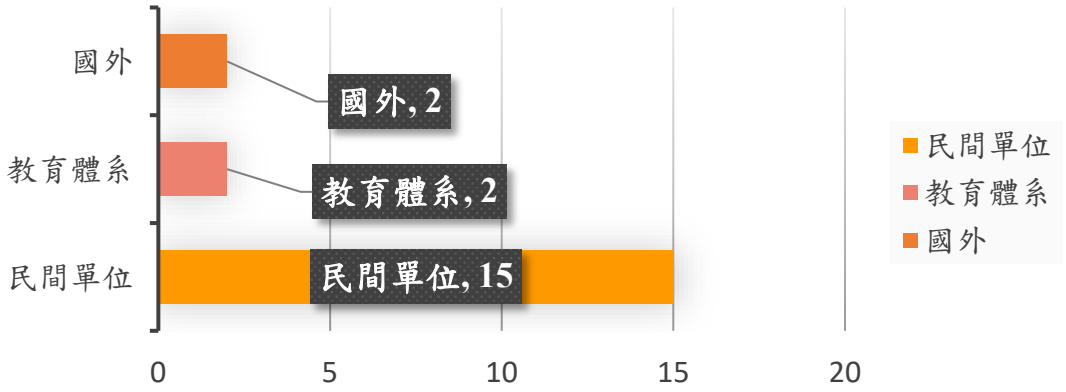


資料來源：本報告整理

圖11 利用漏洞獲取帳密

現場調研發現該網通設備除與 Cisco 設備有共通漏洞外，其系統預設 root 帳密亦雷同，部分機型若有開啟 telnet 服務，駭客亦可使用此組帳密連線入侵。

經分析中繼站現場側錄之封包，發現除政府機關外，尚有其他受駭主機連線報到，而由於機關部分在事前已先透過警訊通知機關應處，故側錄期間未有機關受駭而連線報到，受駭單位類型統計，詳見圖 12。



資料來源：本報告整理

圖12 受駭單位類型統計

觀測自 108 年起 WaterBear 案件比例有逐年增加趨勢，攻擊目標並不限於政府機關，且發現惡意程式運作邏輯雖維持原來模組化特性，亦可見該惡意程式隱蔽性功能之優化。現行因應之防護策略主要以強化受駭主機流量偵測，及早發現異常現象，並配合未知中繼站挖掘，持續追蹤相關情資與樣本，進行溯源預防與阻斷工作。

4. 結論

本季具指標性案例為探討軍事級間諜程式 Pegasus 遭濫用事件，原用於協助追緝可能透過加密通訊軟體逃逸之犯罪者，因具有多元入侵手機之技術，不需透過點擊，即可將間諜程式 Pegasus 安裝於 Android 或 iPhone 手機上。該程式可全時監控手機，且能將用戶個人相關資料傳送至遠端伺服器。第 2 起案例為印尼防疫追蹤 APP 使用之資料庫未妥善進行防護，導致百萬人之 COVID-19 檢測資訊、醫療紀錄及個資等機敏資訊外洩。印尼防疫追蹤 APP eHAC 使用之 Elasticsearch 資料庫配置錯誤，導致資料外洩事件，外洩之資訊包含所有入境印尼與搭乘國內班機之國內外旅客登錄資料，個人姓名、身分證號碼、病毒篩檢結果、住處及其他個人醫療相關資訊等。

國內部分，分析政府資安威脅現況，發現政府機關通報事件類型，以「非法入侵」為主，綜合類型「其他」次之，接續分別為「網頁攻擊」與「設備問題」。針對本季全球與政府所面臨之主要資安威脅，本報告就「共享或免費軟體之資安管理」與「網站設計之資安管理」提出資安防護建議。

資安專題分享主題為 OWASP Dependency-Track，此專案提出一套第三方元件管理工具，工具可用於開發過程中盤點系統元件，並檢測是否具有已知漏洞，可強化 SSDLC 於開發階段之安全性。專題針對 Dependency-Track 元件分析平台進行簡介，並進行概念性驗證。

另外，資安技術研析主題為 WaterBear 攻擊分析，該惡意程式通常先鎖定目標對象是否使用存在 CVE 漏洞之路由器設備，再利用未即時更新或修改預設設定之設備展開攻擊，取得該路由器控制權後，展開橫向入侵與攻擊活動。鎖定對象除政府機關與民間企業外，亦包含機關之資通服務供應商，藉由入侵其資通系統後，做為跳板再成功滲透政府機關。

資安相關活動

本季行政院資通安全處辦理之資安相關活動，說明如下：

◆ 110 第 1 次政府資通安全防護巡迴研討會

因疫情影響，110 第 1 次政府資通安全防護巡迴研討會採線上方式辦理，議題包含政府資安威脅與防護重點、資通安全管理法施行檢討與宣導事項及資安監控有效性驗證。

政府資安威脅與防護重點，說明 110 上半年通報事件類型，以「非法入侵」為大宗，次之為「設備問題」與「網頁攻擊」，另外 3 級資安事件通報以資料外洩與核心業務中斷為主要資安事件。資通安全管理法施行檢討與宣導事項，包含資安維護計畫、資安事件通報、資安稽核作業及攻防演練實施情形，以及資安弱點通報機制與端點偵測及回應機制等推動作業，並宣導強化委外契約管理機制等事項。資安監控有效性驗證，概述政府領域聯防監控收容架構、SOC 監控有效性驗證、現況及防護建議等事項。

◆ N-ISAC 會員會議

因疫情影響，N-ISAC 會員會議採線上會議辦理，報告事項除 N-ISAC 情資分享執行情形外，亦針對情資格式改版作業進行說明與討論，規劃將現有情資格式升級至 STIX 2.1，同時參考國際組織之情資分類，進行情資類型調整，以利接軌國際資安情資。

本次專題分享之主軸為「強化遠端存取管控與委外安全管理，以提升供應鏈安全」，透過近期資安事件案例，探討遠端存取作業之必要管控措施，同時藉由政府機關委外廠商資安事件中學習，加強委外廠商之監督與管理，強化委外契約與安全管控機制，並落實「原則禁止、例外允許」之遠端存取控管，以強化供應鏈資安防護。