財團法人台灣網路資訊中心因公出國人員報告書

108 年 6 月 4 日

報告人 姓　名	丁綺萍 林穎平	服務單位及職稱	副執行長 網資組 工程師
出國期間	108 年 5 月 20 日 至 108 年 5 月 25 日	出國地點	美國 維吉尼亞州
機密等級	□　機密　□ 密　■一般		
出國事由	報告書內容應包含： 一、出國目的 二、考察、訪問過程 三、考察、訪問心得 四、建議意見 五、其他相關事項或資料 （內容超出一頁時，可由下頁寫起）		
授權聲明欄	本出國報告書同意貴中心有權重製發行供相關研發目的之公開利用。 授權人：　　（簽章）		

附一、請以「A4」大小紙張，橫式編排。出國人員有數人者，依會議類別或考察項目，彙整提出報告。

註二、請於授權聲明欄簽章，授權本中心重製發行公開利用。

出國報告(出國類別：開會)

CNA Summit

出國報告

計畫名稱：強化台灣電腦網路危機處理暨協調中心計畫

受委託單位：財團法人台灣網路資訊中心

出差國家：美國

出國人員：丁綺萍、林穎平

出國期間：中華民國 108 年 5 月 20 日至 5 月 25 日

出國經費：268,825 新台幣

報告日期：中華民國 108 年 6 月 5 日

註：如屬限閱或機密之報告，應於封面加註「限閱」或「機密」字樣，並註明限閱年數或解密條件。

摘要

本中心於 2018 年起參與美國 MITRE 之通用漏洞揭露（Common Vulnerabilities and Exposures, CVE）計畫，並成為管理 CVE ID 的單位（CVE Numbering Authorities，CNA），期望能夠透過該計畫在資安領域的影響力，吸引一般資安單位與獨立資安研究人員主動將漏洞資訊提報給本中心，並於第一時間通報受該漏洞影響的單位與產品提供者，將可能遭受的衝擊降到最低。

本次參與 CNA Summit，旨在了解目前其他 CNA 組織的作業流程與未來 CVE 計畫的改變方向，並藉此機會與其他組織多加交流，建立聯繫管道，拓展未來合作的可能性。

目錄

表目錄

圖目錄

壹、出國目的

本次出國為代表台灣電腦網路危機處理暨協調中心（Taiwan Computer Emergency Response Team / Coordination Center，以下簡稱 TWCERT/CC）前往美國維吉尼亞州由 MITRE 公司針對 CVE 管理單位（CVE Numbering Authorities，以下簡稱 CNA）所舉辦的 CNA Summit。

圖 1：林穎平工程師與丁綺萍副執行長

Common Vulnerabilities and Exposures（以下簡稱 CVE）是一個已知資安漏洞的通用編號清單。於 1999 年由 MITRE 公司發起，以往不同企業間針對漏洞的處理，通常是使用自己內部的編號與描述方法，並沒有一個可以快速且容易的查詢方法。而 CVE 的特點就是提供所有企業一個通用的編號與格式標準，降低不同企業對同一弱點的處理成本、並提高使用者查詢漏洞的效率。

CVE 是一個針對全世界的資安社群專案，任何人都可以查詢 CVE List 上的所有已公開的漏洞。除了 CNA 單位、CVE 董事會與 CVE 贊助單位的

協助之外，全世界亦有許多不同的資安研究單位、企業，透過主動使用 CVE IDs 作為漏洞的主要辨識方法，或是使用其他不同的方式來推廣 CVE 專案。

CNA 單位是 CVE 專案中最重要的一個部分，因為 CNA 單位掌握發放 CVE IDs 的決定權力。本次代表 TWCERT/CC 參與會議主要是要了解目前 CVE 專案的未來走向，以及各個不同工作小組的作業內容與進度，也了解目前專案的執行成果。另一大重點則是趁此機會與其他 CNA 單位交流、建立聯絡管道。

貳、議程安排

時間	議程
08:30 – 09:15	Panel Discussion The current state of CVE and the CNA program
09:15 – 10:15	CVE Rule & Revisions Discussion on the current process for reviewing and revising
10:15 – 10:30	Break
10:30 – 11:00	Working Group Updates Strategic Planning working group
11:00 – 11:30	Working Group Updates Quality working group
11:30 – 12:00	Working Group Updates CNA Coordination working group
12:00 – 13:15	Lunch
13:15 – 14:15	Working Group Updates Automation working group
14:15 – 15:00	Discussion CNA onboarding and management
15:00 – 15:15	Break
15:15 – 16:45	Discussion Open discussion of CVE program
16:45 – 17:00	Wrap-Up

表 1：5 月 22 日議程安排

時間	議程
08:30 – 09:30	CVE Automation and Increasing CVE coverage and Efficiency
09:30 – 10:00	What is acceptable for “Public” disclosure?
10:00 – 10:30	Clarifying the CVE ecosystem
10:30 – 10:45	Break
10:45 – 11:30	Reviewing the CVE appeals process
11:30 – 12:30	Lunch
12:30 – 13:30	Handling end of life products
13:30 – 14:00	Assigning CVEs on third-party products for research and root CNAs
14:00 – 14:30	Lessons learned in becoming a Root CNA
14:30 – 14:45	Break
14:45 – 16:00	Open discussion of CVE program questions and topics
16:00 – 16:30	The future of CVE program summits
16:30 – 17:00	Summit Wrap-Up

表 2：5 月 23 日議程安排

參、議程內容

一、第一日：5 月 22 日

(一) Panel Discussion

此議程主要是在說明目前CVE Program與各個CNA單位的執行情形，2018 年相較於 2017 年，分配的 CVE IDs 增加了 17.6%、共新增了 15 個 CNA 單位。同時也說明了關於後續 CVE Program 的可能發展方向，包含CVE Program內所定義的角色與結構等等。希望能夠藉由一系列的改變提升 CVE Program 對於社會的貢獻，以及盡可能涵蓋所有範圍，並保持一定的擴展性。

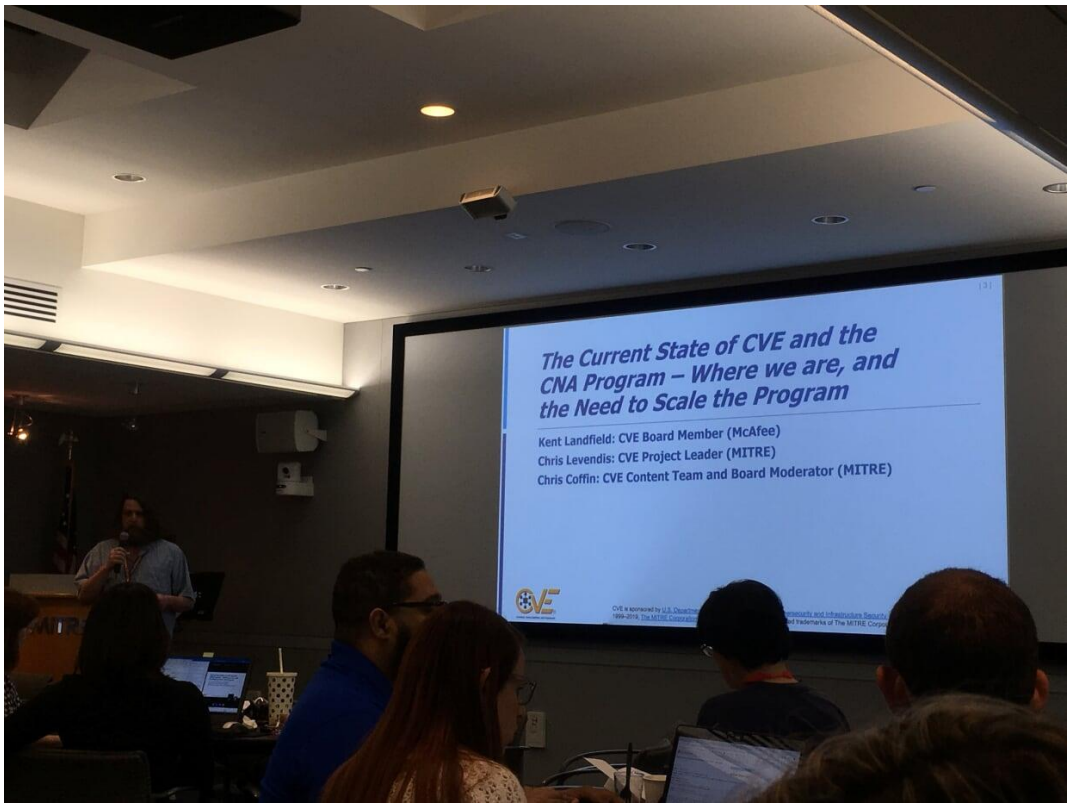

圖 2：Panel Discussion

(二) CVE Rules & Revisions

此議程主要在說明 CVE Program 中各個工作小組的工作範圍，以及說明未來更新 CNA Rules 的方式與流程。預計在 2019 年底會有新版規則的修訂草案。

(三) Working Group Updates

1. Strategic Planning working group

   該工作小組主要是負責 CVE Program 策略與計畫面的作業，在該議程中，工作小組的負責人更詳細的描述 CVE Program 的未來走向與未來的架構，主要是將 MITRE 在 CVE Program 所擁有的權力獨立出來，未來將有獨立的單位負責處理爭議、管理 CVE List 以及發放 CVE IDs 給沒有其他適合 CNA 的漏洞。

2. Quality working group

   負責確保更新上去的 CVE Entry 都有一定的水準，使 CVE Program 能夠對整個社會更有價值。在議程中主要討論到

   (1) 目前必要提供的資訊是否充足

   (2) 哪些資料必須被收集

   (3) 更新速度與品質間的取捨

   (4) SaaS 產品的漏洞

   (5) CVE 的標籤與分類

   (6) 是否要提供統一的版本號標準

3. CNA Coordination working group

   該工作小組主要負責 CNA 單位審核、定義負責區間的業務，並專注於提升 CNA 之間溝通的效率與參與度。

4. Automation working group

   該工作小組主要提供目前 CVE Program 所有自動化的工具。在議程中提到了未來 CVE Program 自動化機制的發展規劃。

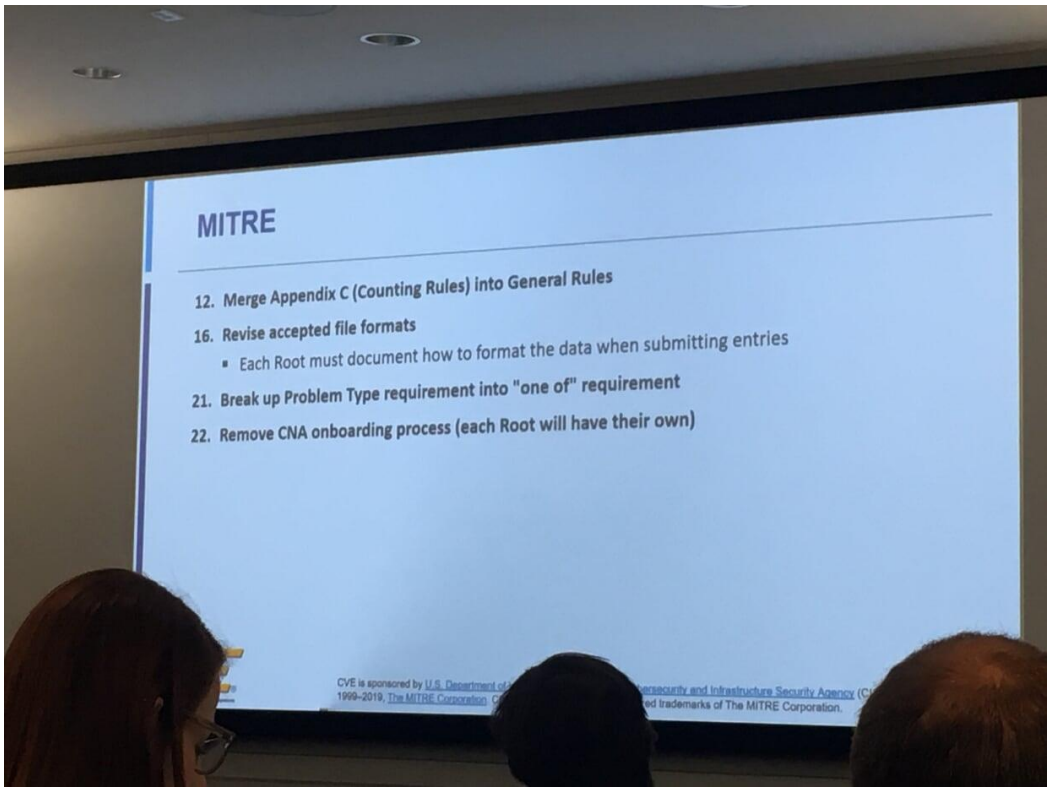

圖 3：Working group updates

(四) CNA onboarding and management

議程前段主要在針對CNA onboarding training的調整作說明，後段則是提到了關於未運作 CNA 單位的處理機制，若 CNA 單位在六個月內沒有任何動作，則會收到來自 MITRE 的通知信，所謂的動作包含：保留 CVE IDs、發布 CVE IDs、參與工作小組、回應通知信。另外也有提到關於 RBP（Reserved But Public，所謂的 RBP 是指相關漏洞已經被公開且也有分配 CVE IDs，但是尚未被更新至 CVE List）的政策，從該政策實施以來，已經降低了 40% 的 RBP 數量。

(五) Discussion

此議程主要是各個 CNA 單位提出一個主題來讓大家討論，第一天的討論主要圍繞在如何推廣 CVE Program，因目前資安研究人員認為能夠得到一個 CVE ID 是一種榮耀，但是對於部份的企業來說，產品若是有一個漏洞被發布了 CVE ID，就有可能會影響企

業的名聲，甚至導致使用者不再購買相關產品，使得部分 CNA 單位在進行求證與通報的過程屢屢遭遇困難。不過也有部份的企業非常看重 CVE Program 所帶來的價值，甚至主動申請成為 CNA 單位。

二、第二日：5 月 23 日

(一) CVE Automation and Increasing CVE Coverage and Efficiency

此議程討論了漏洞與 CVE 的生命週期，並且說明每個階段可以透過哪些方式達到自動化的效果。基本上漏洞的生命週期如下：

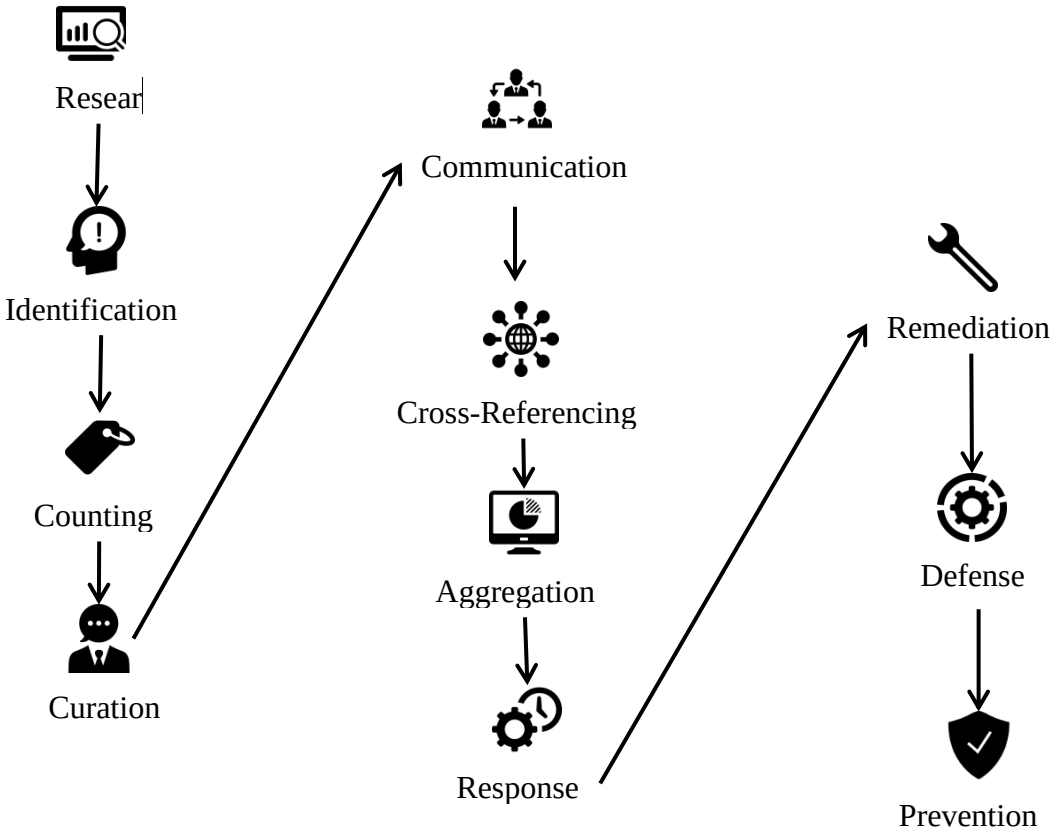

圖 4：Vulnerability/CVE Lifecycle

(二) What is acceptable for “Public” disclosure?

在 CNA 的規範裡有要求任何要申請 CVE ID 的漏洞都必須能夠公開，在本議程中就提到了所謂「公開」的定義。目前可被接

受的有第三方的公開報告、GitHub 或是類似的程式碼代管系統中的 commit、bug tracker 或是公開的 mailing list。議程尾聲也有討論到關於參考資料是否也應提供的議題。

(三) Clarifying the CVE ecosystem

在該議程中，由 Linux Foundation 以及 Rapid 7 的與會者主講，分別由上游（Upstream）開發者與下游（Downstream）的角度來說明目前 CVE Program 在開放軟體界中的一些趨勢與困境。

(四) Reviewing the CVE appeals process

本議程由 Cisco Talos 與 ZDI 的與會者主講，針對當 CNA 單位與產品廠商出現意見分歧時的處理流程做討論。

(五) Handling end of life products

此議程由 TIBCO、ZDI 以及 Microsoft 的與會者主講，在會議前 Microsoft 剛好對已經終止維護的 Windows 版本發布 CVE IDs 以及安全性更新。在議程中，與會者們討論到是否應該對 EOF 發布 CVE IDs 並將其揭露，或是應該低調處理降低遭到有心人士利用的機率。

(六) Assigning CVEs on third-party products for research and root CNAs

此議程由 ZDI、Rapid 7 以及其他與會者主講，在現今的 CVE Program 中有許多是資安研究機構類型與漏洞獎勵類型的 CNA 單位，他們往往需要與產品的廠商取得聯繫，在本議程中，討論了目前 CNA 單位試圖對第三方產品發布 CVE IDs 時所遇到的困境以及解決方法。

(七) Lessons learned in becoming a Root CNA

本議程由 JPCERT/CC 的兩位與會者主講。主要介紹了 JPCERT/CC 的發展簡史以及目前 JPCERT/CC 所涵蓋的範圍與組織架構。主講人也提到目前 JPCERT/CC 的 CVE 分派流程、遇到

的問題以及未來的計劃。

(八) Open discussion / The future of CVE program summits

在本議程中主要談論到了 CNA 單位如何能夠做得更好、擁有更多的互動，除了討論是否舉辦更多實體的討論會之外，也有提到線上會議的可行性，以及 RBP report 的提供等等的議題。

肆、心得與建議（對計畫效益與建議事項）

TWCERT/CC 自 2018 年申請成為台灣產品的 CVE 管理單位，接獲的漏洞通報數量有逐漸增加的趨勢，一開始曾經因為不熟悉處理流程而導致發放 CVE IDs 的進度緩慢，在處理了幾個漏洞之後也逐漸形成一個初步的處理流程，除了提高事件的處理效率之外，也可以更清楚事件的處理進度。

本次能夠參加 CNA Summit 2019 實為非常好的機會，在剛起步的階段就能夠與 JPCERT/CC 以及其他有許多經驗的與會者交流，無疑是對 TWCERT/CC 在 CNA 業務上的一大助力。以下將就本次參加 CNA Summit 2019 的經驗，提供建議。

一、增加台灣廠商對於漏洞揭露的正向看法

在會議中有數次討論到目前還是有許多的廠商認為自家產品被指派一個 CVE ID 之後，就等同於被貼上了不安全的標籤，然而對於資安研究人員來說，自己所通報的漏洞能夠被賦予一個 CVE ID 則是無上的榮耀。我們如何能夠將類似的正向看法提供給台灣廠商，藉以提升廠商的配合度，是今後必須要討論的課題。

二、提供更多元的漏洞通報方式

目前 TWCERT/CC 所採用的通報流程需要通報者先於台灣漏洞紀錄平台（https://tvn.twcert.org.tw）上下載一個 txt 範本檔案，並在填寫相關資料之後透過電子郵件的方式通報，曾經有合作單位表示其過程

太過繁瑣，是否能夠提供其他的方式通報。未來或許可以新增像是網頁通報或是 API 的方式供合作單位使用，提高事件的通報效率。

三、增加英文版 TVN 頁面

目前CVE Entry只允許透過英文撰寫,而TVN平台內容為全中文，英文版的內容則是於英文版的官方網站公開，若 TVN 平台能夠同時提供相同介面的英文版內容，將會使整個平台看起來更加完整。