TLP:WHITE

台灣資安漏洞發布之現況與未來

Announcement Advisory Report (ANAR)

2018-05-08

TWCERTCC-ANAR-2018005

TLP:WHITE

Summary

- 現今網路安全議題上最常被使用的已知漏洞資料庫為「通用漏洞揭露」(Common Vulnerability and Exposures, CVE)平台，它收集各種資安漏洞及漏洞並給予編號，以便公眾查閱。CVE 是由美國國土安全部網路安全和通信辦公室贊助，非營利組織 MITRE 公司所營運維護，漏洞編號是由「漏洞編號授權單位」(CVE Numbering Authorities, CNA)負責漏洞審核與編號賦予。

- TWCERT/CC 已向 MITRE 申請成為台灣之漏洞編號授權單位－Root CNA，協助 MITRE 審核及分配台灣廠商設計開發的資通訊軟、韌體產品所通報資安漏洞的 CVE ID，可在漏洞訊息尚未揭露下，協助台灣廠商早期掌握與及時漏洞修訂。

Description

現今網路上最常使用的資安漏洞資料庫，是由美國 MITRE 公司負責營運維護的「通用漏洞揭露」(Common Vulnerability and Exposures, CVE)平台，CVE 為美國國土安全部網路安全和通信辦公室所贊助的計畫。當資通訊產品之軟、韌體被發現運算邏輯等影響機密性、完整性或可用性的設計缺失時，得以透過 CVE 平台，將所有已知漏洞資訊和安全風險的名稱標準化，並賦予漏洞編號。截至 2018 年 4 月，CVE 共有來自 14 個國家(澳大利亞、奧地利、加拿大、中國、法國、德國、以色列、日本、荷蘭、俄羅斯、南韓、台灣、英聯合王國、美國)的 87 個漏洞編號授權單位參與。

CVE 漏洞審查與編號分配需由經 MITRE 公司核可的「漏洞編號授權單位」執行。為了讓每一個 CNA 彼此在溝通、管理及發布漏洞時能有一致的標準，MITRE 制定「漏洞編號授權單位規章」(CVE Numbering Authorities (CNA) Rules)[1]，將「漏洞編號授權單位」分為三種類別，分別就其所負責維護管轄之範疇，進行 CVE 審核及編號分派。CNA 之組織架構如圖 1 所示，說明如下：

1. 主漏洞編號授權單位(Primary CNA)：亦即 MITRE 公司，負責授予 Root CNA CVE 編號區段、維護整體 CVE 編號清單並且對外公布，同時也擔任各個 Root CNA 間溝通管道。

2. 根漏洞編號授權單位(Root CNA)：擔任 Primary CNA 與 Sub CNA 間的協調者，協助 Primary CNA 維護所轄範圍內產品，供應商或產品的 CVE 審核與編號分派發布作業，且有義務主動告知 Primary CNA 其所發布之漏洞資訊更新。Root CNA 通常是由地區的協調中心或特定領域資訊分享與分析中

心擔任，例如電腦網路危機處理小組 (Computer Emergency Response Team, CERT)、資訊分享與分析中心 (Information Sharing and Analysis Center, ISAC)或是發展成熟的研究機構。

3. 子漏洞編號授權單位(Sub CNA)：Sub CNA 通常由產品開發商擔任，通常是擁有明顯的客戶群且已具備資訊安全顧問諮詢能力的廠商，負責自身產品相關的漏洞維護作業。Sub CNA 對於發布之漏洞有資訊更新，應主動告知 Root CNA。而目前已成為 CNA 之單位列舉部分於表 1 中，詳細可參閱[2]。

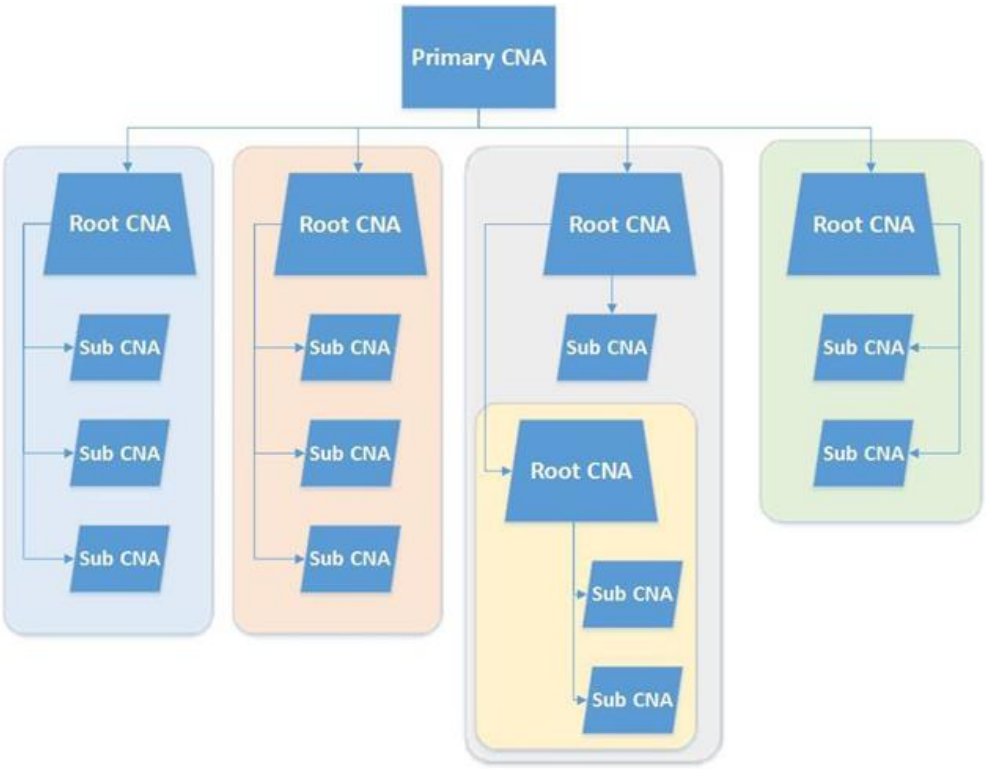

圖 1. CNA 組織架構圖

表 1. CNA 列表

CNA 種類	數量	單位名稱
Primary CNA	1	MITRE Corporation
Root CNA(含 National CERT and Industry CERTs)	5	CERT/CC, ICS-CERT, Distributed Weakness Filing Project, JPCERT/CC, KrCERT/CC
Sub CNA(含 Vendors and Projects,	81	包含 Apple Inc., Adobe Systems Incorporated, Android (associated with

Vulnerability Researchers, Bug Bounty Programs)		Google Inc. or Open Handset Alliance), Apache Software Foundation, ASUSTOR Inc., Facebook, Kaspersky Labs, QNAP Systems Inc., Synology Inc., Trend Micro, Inc.等。

根據MITRE的「漏洞編號授權單位規章」,漏洞發布運作流程分為五個步驟，依序為申請 CVE ID 區段、CVE ID 保留、CVE ID 分派、CVE 通報及 CVE 發布(如圖 2 所示)。TWCERT/CC 將依據前述漏洞發布運作流程，成為台灣資通訊產業之漏洞揭露服務提供者。

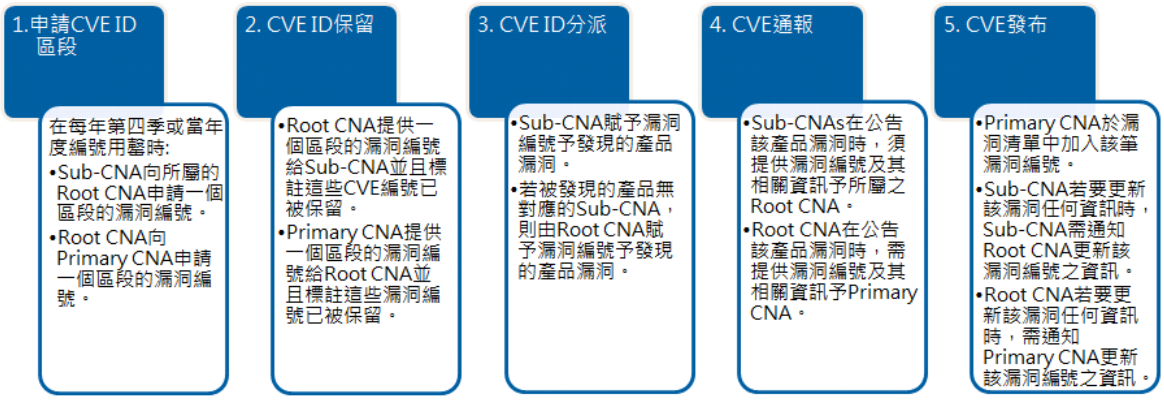

圖 2. 漏洞發布運作流程

舉例來說，當 CNA 接收到資通訊產品被發現存在漏洞時，首先會評估該漏洞是否有主責的 CNA。若有，則將此漏洞提供予該產品主責之 CNA 進行漏洞審核作業、編號分派與發布；若無主責 CNA，則逕由接收到訊息之 CNA 或 MITRE 依漏洞編號發布流程進行處理。

目前台灣有三家資通訊產品廠商為 Sub CNA，分別是群暉科技 (Synology Inc.)[3]、威聯通科技(QNAP Systems, Inc.)[4]及華芸科技(ASUSTOR Inc.)[5]，均可處理與發布該公司產品所發現的漏洞編號，其餘台灣廠商的產品漏洞則多由其他國際 CNA 處理漏洞發布作業。台灣資通訊產業發達，素有科技島之稱，所研發販售之資通訊產品已在國際市場上廣為銷售，為協助台灣廠商重視 CNA 漏洞發布機制，提升產品的安全性，爰此，TWCERT/CC 將透過申請成為 Root CNA，協助我國資通訊產品漏洞的審核及漏洞編號發布，來協助相關廠商掌握其產品漏洞並及早修訂。

依 MITRE 之 CVE 漏洞編號賦予規定，TWCERT/CC 會於每年第四季，向 MITRE 申請隔年度將使用的 CVE ID 區段，來保留給台灣廠商使用。這些 CVE ID 除了分配給前述三個台灣 Sub CNA 使用之外，若 TWCERT/CC 接獲其它台灣廠

商之軟、韌體產品漏洞情資，且該產品並無適當的 CNA 主責時，TWCERT/CC 將擔任與軟、韌體製造商之間的協調窗口，積極通報該產品廠商相關漏洞資訊並提醒進行漏洞修補，以利廠商維護其產品的品質與商譽。在確認接獲通知之廠商已確實掌握該漏洞情資後，TWCERT/CC 也將協助審核此漏洞情資與相關修訂情形，並賦于 CVE ID 及漏洞發布。

若由台灣的 Sub CNA 或 TWCERT/CC 所協助審核之漏洞有任何資訊更新，如最新的漏洞修補建議與版本等，本中心亦將協助提供漏洞內容更新予 MITRE，以維護 CVE 計畫漏洞揭露資料庫之全球一致性。

Recommendations

針對國內外所發現有關台灣廠商所開發之資通訊產品漏洞發布作業，TWCERT/CC 提出「漏洞處理框架(Vulnerability Handling Framework)」，以確保國內外資安研究機構、漏洞懸賞計畫或其他 CERT/CSIRT 組織在發現台灣產品疑似存在相關資安漏洞時，能夠有漏洞通報管道及負責發布漏洞編號的單位(如圖 3 所示)。

當 TWCERT/CC 接獲國內某產品存在新資安漏洞之通報後，若該漏洞符合 MITRE 所定義之漏洞規則，TWCERT/CC 將循「漏洞處理框架」，將漏洞相關資訊通報該產品廠商，待廠商研擬出安全更新或緩解措施後，TWCERT/CC 會協助進行此漏洞審查及編號賦于，最後將於 CVE 漏洞資料庫進行更新發布。

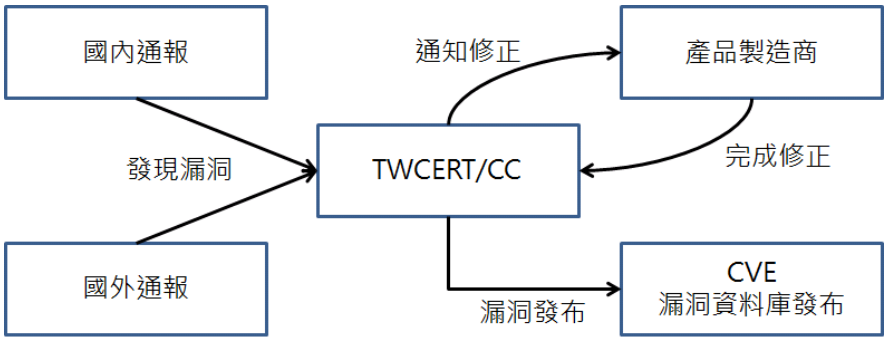

圖 3. 漏洞處理框架

當今企業不僅需要提供各種多元的服務與應用，更得對抗日趨複雜的資安威脅。TWCERT/CC 鼓勵台灣資通訊產品開發商致力於增進其產品的安全性，建議產品開發商應該積極的看待漏洞發布機制，及時修補所發現之產品漏洞，並通知使用者進行更新，讓使用者享受產品功能之餘，不用擔心產品漏洞遭利用而進一步引發資安事件。

References

[1] MITRE Cooperation. (2018, January 1). "Common Vulnerabilities and Exposures (CVE) Numbering Authority (CNA) Rules Version 2.0", Retrieved May 7, 2018, from the World Wide Web: https://cve.mitre.org/cve/cna/CNA_Rules_v2.0.pdf

[2] MITRE Cooperation. (2018, April 27). "Request CVE IDs", Retrieved May 7, 2018, from the World Wide Web: https://cve.mitre.org/cve/request_id.html

[3] Synology Inc. "對資訊安全的持續承諾", Retrieved May 7, 2018, from the World Wide Web: https://www.synology.com/zh-tw/company/news/article/CNA_join/%E5%B0%8D%E8%B3%87%E8%A8%8A%E5%AE%89%E5%85%A8%E7%9A%84%E6%8C%81%E7%BA%8C%E6%89%BF%E8%AB%BE

[4] QNAP Systems, Inc. (2017, August 31). "QNAP 獲得授權參與 CNA 計畫，保護資安不遺餘力", Retrieved May 7, 2018, from the World Wide Web: https://www.qnap.com/zh-tw/news/2017/qnap-%E7%8D%B2%E5%BE%97%E6%8E%88%E6%AC%8A%E5%8F%83%E8%88%87-cna-%E8%A8%88%E7%95%AB-%E4%BF%9D%E8%AD%B7%E8%B3%87%E5%AE%89%E4%B8%8D%E9%81%BA%E9%A4%98%E5%8A%9B

[5] Asustor Inc. "New CNA - Asustor", Retrieved May 7, 2018, from the World Wide Web: https://cve.mitre.org/data/board/archives/2017-10/msg00026.html