TWCERT/CC 漏洞揭露政策

2.1 版

112 年 11 月 8 日

聲 明

本文件之交通燈號協議(Traffic Light Protocol, TLP)為白色燈號(TLP: CLEAR)，無揭露限制，為可對外公開之內容。當資訊具有最小或沒有可預見之誤用風險時，資料可以被標註為白色燈號，透過公開發布之規則即可讓此份文件對外發布。接收方取得此份資料時，透過一般發布資訊之流程，亦可對外公開此資訊。

目錄

圖目錄

第 1 章、簡介

台灣電腦網路危機處理暨協調中心(Taiwan Computer Emergency Response Team / Coordination Center，TWCERT/CC，以下稱本中心)現由台灣網路資訊中心營運，並在行政院資通安全處指導下運作。

為了提升我國整體資安防護能量，本中心主導推動資安事件通報，並透過與國內外 CERT/CSIRT、資安組織、學研機構、民間社群、政府單位及私人企業等多元化合作，並進行資源整合。

做為可信的漏洞通報中介單位，本中心自 2018 年起參與美國 MITRE 之通用漏洞揭露(Common Vulnerabilities and Exposures, CVE®)計畫[1]，申請成為 CVE 編號管理者(CVE Numbering Authorities, CNA)，並建置台灣漏洞紀錄(Taiwan Vulnerability Note, TVN)平台，透過協助國內外廠商處理產品漏洞，以儘快完成漏洞緩解及修補，避免有心人士利用產品漏洞造成使用者遭駭之情況發生。

以上的努力，均為共同維護台灣整體網路安全穩健，從安全、便利、效能三面向來推動資通安全，以逐步實現建構網路安全環境之願景。

[1]更多資訊請參考 CVE 計畫網站：https://cve.mitre.org/

第 2 章、漏洞通報方式

漏洞通報者可將漏洞細節報告及相關佐證資料寄至 cve@cert.org.tw，本中心將於接獲資料後進行後續處理流程。

若欲使用PGP KEY 先行將檔案加密再寄給本中心，請使用本中心公開之PGP KEY(網址：https://www.twcert.org.tw/tw/cp-26-75-6ad16-1.html, KeyID：1E9D1F1B)。

第 3 章、漏洞揭露方式

本中心之漏洞揭露及處置方式，係根據 CVE®官方所公布之 CVE 編號管理規則(https://cve.mitre.org/cve/cna/rules.html)及中華民國法律規定。下述各項規範若有說明不足處，TWCERT/CC 保留最終解釋權。

3.1 、名詞定義

3.1.1 、程式錯誤(Bug)

由於程式中運算邏輯上的流程或設計錯誤，導致程式執行後所得到之結果並非預期結果，稱之為程式錯誤(Bug)。

3.1.2 、漏洞(Vulnerability)

漏洞(Vulnerability)之定義為發生於軟體、韌體及微程式中的 Bug，且若此 Bug 遭利用，會導致資料的機密性、完整性或可用性產生負面影響。因此，若為硬體零件設計不良導致產品外殼損毀等，則不可稱之為漏洞。

3.1.3 、漏洞緩解(Mitigation)

漏洞緩解(Mitigation)之定義為，透過修改程式碼來消除漏洞，但若以變換、降低軟韌體功能之規格等方式消除漏洞，則不稱做漏洞緩解，例如直接將含有漏洞之功能或通訊埠移除，則不可稱之為漏洞緩解。

3.1.4 、漏洞通報者

將所發現之產品漏洞細節及相關證據提供本中心之人員。

3.1.5 、產品廠商

開發出含有漏洞之產品之產品製造商。

3.1.6 、通用漏洞揭露(CVE)

通用漏洞揭露(Common Vulnerabilities and Exposures, CVE)為一個記錄已知產品漏洞之資料庫，資料庫中記錄產品廠商、產品名稱、漏洞描述及參考來

源等。此資料庫目前由美國非營利組織 MITRE 所營運維護，且於全世界被廣為使用，其中亦包含美國官方資安單位等。

3.1.7 、CVE 編號(CVE ID)

每個記錄在 CVE 中的漏洞皆會被發放一個獨特編號，以利引用時可代表特定漏洞，該編號則被稱作 CVE 編號(CVE ID)，亦可稱做「CVE Entry」、「CVE」或「CVE number」，且其格式為 CVE-YYYY-NNNN，N 的部分至少 4 碼，最長則無限制，例如 CVE-2017-0144，此 CVE ID 代表的則是 2017 年造成嚴重感染事件之 WannaCry 勒索軟體，攻入目標主機時所使用之漏洞。

3.1.8 、CVE 編號管理者(CNA)

CVE 編號管理者(CVE Numbering Authority, CNA)為一志工組織，可為來自世界各國之國家 CERT、產業 CERT、研究機構、漏洞提報組織或廠商等。每個 CNA 都有不同的權責範圍，並有權限可以對權責範圍內之產品漏洞發布 CVE ID，以及後續對 CVE ID 的內容進行維護。

CNA 分為主要 CNA(Primary CNA)、根 CNA(Root CNA)及一般提到 CNA 時所指的次要 CNA(Sub CNA)等，其中主要 CNA 之權責範圍大於根 CNA，根 CNA 之權責範圍又大於次要 CNA，且次要 CNA 須透過根 CNA 來與主要 CNA 進行協調。

上屬 CNA 除須協調下屬 CNA，並提供其教育訓練、審核新加入之 CNA 之外，並須確認下屬 CNA 之權責範圍。若次要 CNA 無法找到一個對應的上屬根 CNA，則可往上追溯至上一層之根 CNA 或主要 CNA。

主要 CNA 為維運 CVE 之 MITRE 公司，除一般 CNA 事務外，亦負責 CVE 專案全般事項；根 CNA 為各國家下屬 CERT/CSIRT 或領域 ISAC，次要 CNA 則為廠商。另由於並非每個國家或其領域都有根 CNA，因此 MITRE 公司除身為主要 CNA 外，同時也是根 CNA，供無上屬根 CNA 之次要CNA 可將 MITRE 公司視作根 CNA，以利各項事務推動。

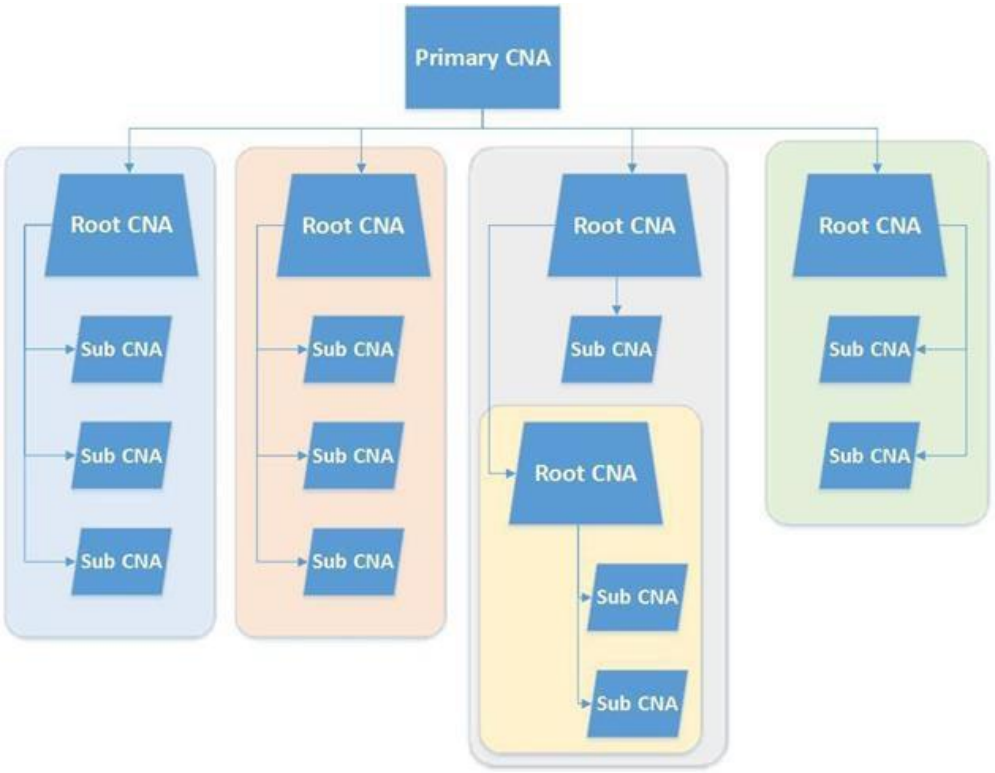

圖 1、CNA 架構圖 [2]

3.1.9 、共用程式庫(Shared Codebase)

程式庫(Codebase)指的是一個程式碼資料庫，內含分別可執行不同功能之程式碼，並可利用這些程式碼來組成系統、應用程式或軟體元件。若程式庫中程式可以於多個產品中引用並使用，則稱其為共用程式庫(Shared Codebase)。

3.2 、漏洞報告公開時程

任何通報至本中心之漏洞報告，將於通報日期起 90 個日曆天內公開報告之基本資料，包含主旨、公開日期、影響產品、簡要描述、通報人等資訊，例如於 2019 年 8 月 13 日接獲通報，則最晚於 2019 年 11 月 11 日公開。

漏洞報告中所闡述之詳細漏洞利用方式等技術細節，則於該漏洞有明確漏洞緩解方式、廠商已公告修補版本，或確認該報告提及之漏洞無須處理後公開，不設定強制公開時間。

本中心有權利可於判斷漏洞影響程度後，決定是否延後各項資訊之公開時程，以及公開內容之詳細程度。

3.3 、漏洞資訊揭露位置

本中心開發台灣漏洞紀錄(Taiwan Vulnerability Note, TVN)平台，將於此平台中提供漏洞通報紀錄，包含公開日期、影響產品、問題描述、解決方法、相關 CVE ID、相關連結、漏洞通報者等資訊。

3.4 、漏洞報告處置流程

本中心於接獲漏洞通報後之處置流程如圖 2 所示。漏洞通報者發掘漏洞，並通報漏洞技術細節至本中心，本中心接獲漏洞通報後，首先進行初步判斷，確認漏洞報告之內容是否足夠，若尚有缺漏處則請漏洞通報者補充，確認無須補充後，本中心發放此漏洞通報一 TVN 編號，並於 90 個日曆天內於 TVN 平台中公布漏洞基本資訊。

接著，本中心將漏洞報告提供產品廠商，由產品廠商確認漏洞資訊，本中心則協助產品廠商及漏洞通報者傳遞漏洞資訊、漏洞修補結果驗證之確認訊息。

最後，待三方皆確認漏洞修補完成或有相對應漏洞緩解方法後，本中心將把漏洞技術細節公布於 TVN 平台中。

若接獲之漏洞報告資訊有下述情況，本中心有權決定暫停或停止處理該份報告：不足以確認漏洞內容或發生原因、違反官方 CVE 編號管理規則(CVE Numbering Authorities(CNA) Rules)、無法聯繫漏洞通報人釐清細節等。

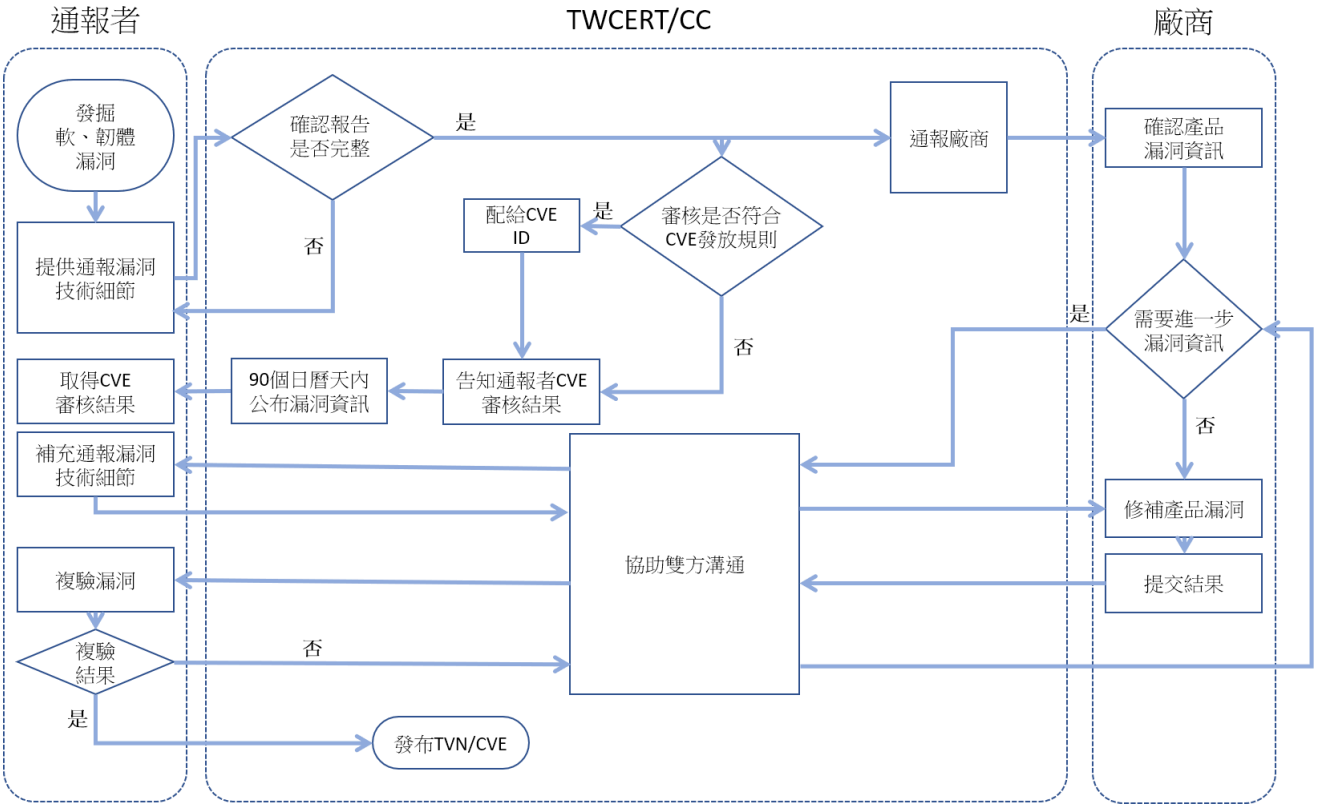

圖 2、漏洞報告處置流程

3.5、CVE 編號發放規則

若在漏洞報告處理流程中，漏洞通報者、本中心或是產品廠商對於所發現的漏洞欲申請 CVE 編號，將由本中心主責確認是否通過官方定義之 CVE 編號發放規則，如圖 3 所示。一旦確認符合申請 CVE 編號之資格，且產品廠商也回覆確認漏洞資訊，本中心將發放 CVE 編號給該漏洞。

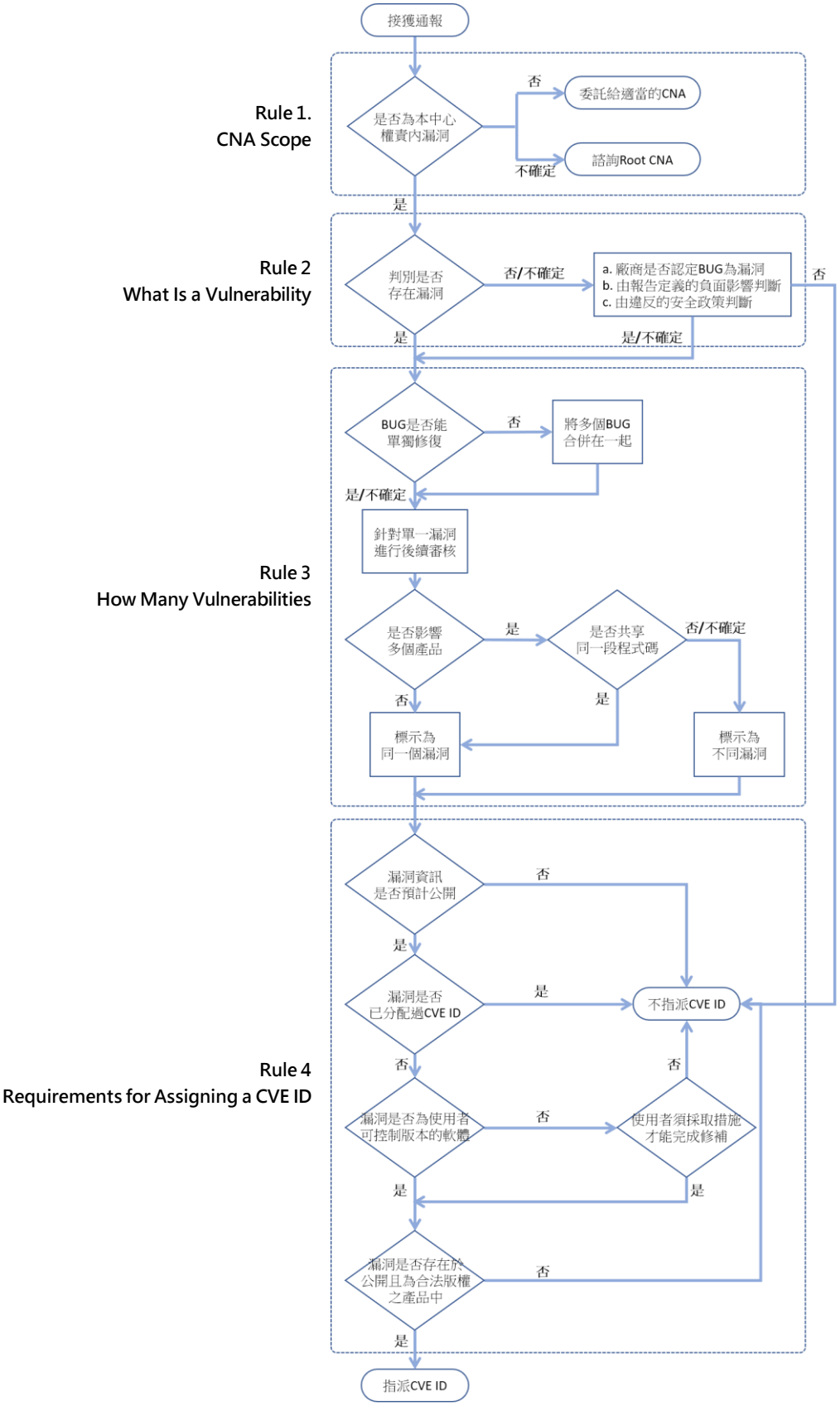

圖 3、CVE ID 發放規則

CVE 編號發放規則包含四個Rules，皆符合後，才能確認其中包含幾個漏洞，以及每個漏洞是否可發放 CVE 編號，也就是說，有可能會有無法發放 CVE 編號給某一漏洞的狀況發生。各項判斷介紹如下：

3.5.1 、Rule 1：CNA Scope

- 由於每個 CNA 皆有不同的權責範圍，因此在欲發布漏洞前，須確認該漏洞涵蓋在哪個 CNA 的權責範圍內，並由該 CNA 對該漏洞發布 CVE ID。
- 若找不到可以直接負責的次要 CNA，可將漏洞轉交其上層之根 CNA。
- 每個漏洞可由多個 CNA 共同合作來處理。
- 若漏洞範圍包含多個 CNA，則須由 Root CNA 協調處置方式。
- 如果不確定漏洞為哪個 CNA 之權責範圍，則可洽詢根 CNA。

3.5.2 、Rule 2：What Is a Vulnerability

- 確認包含Bug 之產品所屬之產品廠商，並判別該 Bug 是否為漏洞。
- 產品廠商確認該 Bug 為會對產品造成負面影響的漏洞。
- 若產品廠商不願意確認或不確定該 Bug 為會對產品造成負面影響的漏洞、產品廠商不願意支援該產品漏洞修補，可透過漏洞通報者的報告，或是該 Bug 是否違反產品廠商之產品安全政策，進而判斷該 Bug 是否為會對產 品造成負面影響的漏洞。

3.5.3 、Rule 3：How Many Vulnerabilities

- 每 個Bug 必須可以在不修復其他 Bug 的狀況下單獨被修復。
- 如果在修復Bug A 時也會同時修復 Bug B，請將 Bug A 及Bug B 合併成 Bug A。若不確定單個或多個 Bug 是否能單獨被修復，則視為一個 Bug 處理。

針對單一漏洞進行審核：

- 僅影響單一產品，則標示為同個漏洞。
- 若多個產品中皆使用同一段程式碼，則為這些產品標示成同個漏洞。
- 影響多種產品，但引用的程式碼不同，則為每個產品標示成不同漏洞。不確定或未定義，則為每個產品標示成不同漏洞。

若該漏洞因為使用含有漏洞的函式庫、協定或標準：

- 產品所引用之程式庫因符合特定規格而導致漏洞，則為該函式庫、協定或標準標示成同個漏洞。
- 產品所引用之程式庫因實作函式庫、協定或標準而導致漏洞，則為每個受影響的程式庫標示成同個漏洞。
- 如果不確定，則為每個受影響的程式庫標示成不同漏洞。

3.5.4 、Rule 4：Requirements for Assigning a CVE ID

Rule 4.1：漏洞資訊是否預計公開

- 若欲發放一 CVE ID 給一漏洞，此漏洞之基本資訊必須要公開在一個可存取的URL 中，基本資訊包含產品名稱、版本、及問題類型(漏洞類型或影響)。
- 該 URL 內的資訊在免費註冊和登錄後才能免費觀看是可以被接受的，但不能有其他限制。若進一步詳細技術資訊需要付費才能觀看，則該漏洞亦可視為公開。

Rule 4.2：確認 CVE 中無相同漏洞存在

- 至官方 CVE 列表(網址：https://cve.mitre.org/index.html)中確認漏洞是否已經存在 CVE ID，若已存在則不再發放 CVE ID。

Rule 4.3：漏洞是否為使用者可控制版本的軟體

- 若受漏洞影響之產品或服務版本為使用者可控制，則發放 CVE ID。
- 若產品或服務之版本不受使用者控制，但該漏洞需要使用者採取措施才能解決，亦會發放 CVE ID。
- 若使用者無法對有漏洞的產品採取任何緩解措施或修復程序，則無法發放 CVE ID 給該漏洞，如線上網站(例如 Google.com) 及軟體即服務(Software-as-a-Service, SaaS)等，此類產品就算出現漏洞也無法發放 CVE ID。
- 若產品雖為 SaaS，但仍有安裝在少數客戶端上的軟體存在漏洞，則仍會發放此產品該漏洞的 CVE ID；若漏洞同時影響 SaaS 版和客戶端安裝版，亦會發放 CVE ID。

Rule 4.4：漏洞是否存在可公開存取即有合法版權之產品中

- 若漏洞存在未公開或未獲得許可之產品，則不發放 CVE ID。
- 僅有可被公開存取且有合法版權產品內含之漏洞才可發放 CVE ID，若僅於單一企業內部使用之軟體或惡意程式含有漏洞，皆不可發放 CVE ID。
- 非正式版產品，如已停止更新的測試版軟體，以及在新版本軟體發布前提交的修復版本中若含有漏洞，則不可發放 CVE ID。

3.6、漏洞通報者稱呼及聯繫方式公開

本中心於公開漏洞通報紀錄時，會一併將漏洞提報者之稱呼公開，該稱呼可為，且不限於暱稱或單位名稱等，以確保發掘漏洞的功勞可歸功於此漏洞通報者，若漏洞通報者不希望稱呼被公開，可於任何時間告知本中心，本中心將協助修改並顯示為匿名。

本中心擔任漏洞通報者與產品廠商間的協調者，協助雙方確認漏洞細節及修補進度等事項，若產品廠商在接獲漏洞報告後需要對漏洞通報者進一步詢問細節，本中心將先行詢問漏洞通報者是否願意提供電話或電子郵件等聯繫方式至產品廠商，若是，則將由產品廠商直接聯繫漏洞通報者以確認漏洞細節，惟仍須告知本中心漏洞修補狀況，以利更新漏洞報告資訊；若否，產品廠商則無法直接聯繫漏洞通報者，並由本中心擔任產品廠商及漏洞通報者間溝通橋樑。

第 4 章、連絡方式

若對於此份文件或是本中心有任何疑問或建議，歡迎您不吝指教，並可以下列任一方式連絡本中心。

- 官方網站： https://www.twcert.org.tw/
- 一般連絡： twcert@cert.org.tw
- 漏洞通報： cve@cert.org.tw
- 事件通報： https://www.twcert.org.tw/tw/sp-geno-guide-1.html

第 5 章、參考資料

[1] Common Vulnerabilities and Exposures. ”Common Vulnerabilities and Exposures”, Retrieved April 13th, 2021, from the World Wide Web: https://cve.mitre.org/

[2] CVE Numbering Authorities(CNA) Rules, “CVE Numbering Authorities(CNA) Rules”, Retrieved April 13th, 2021, from the World Wide Web: https://cve.mitre.org/cve/cna/rules.html

[3] CERT Vulnerability Disclosure Policy, “Vulnerability Disclosure Policy”, Retrieved April 13th, 2021, from the World Wide Web: https://vuls.cert.org/confluence/display/Wiki/Vulnerability+Disclosure+Policy