1. 向 TWCERT/CC 通報漏洞方式

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)。

2. 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://www.cve.org/ResourcesSupport/AllResources/CNARules) 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。

2.1 名詞定義

2.1.1 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)。

2.1.2 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。

2.1.3 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。

2.1.4 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。

2.1.5 產品廠商

開發出含有漏洞之產品之產品製造商。

2.1.6 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。

2.1.7 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 CVEYYYY-NNNN，N 的部分至少 4 碼，最長則無限制。

2.1.8 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。

2.1.9 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)。

2.2 漏洞報告公開時程

本中心在確認完報告內容完整性之日期起 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 2025 年 1 月 1 日通報廠商，則最晚於 2025 年 4 月 1 日公開。

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。

2.3 漏洞資訊揭露位置

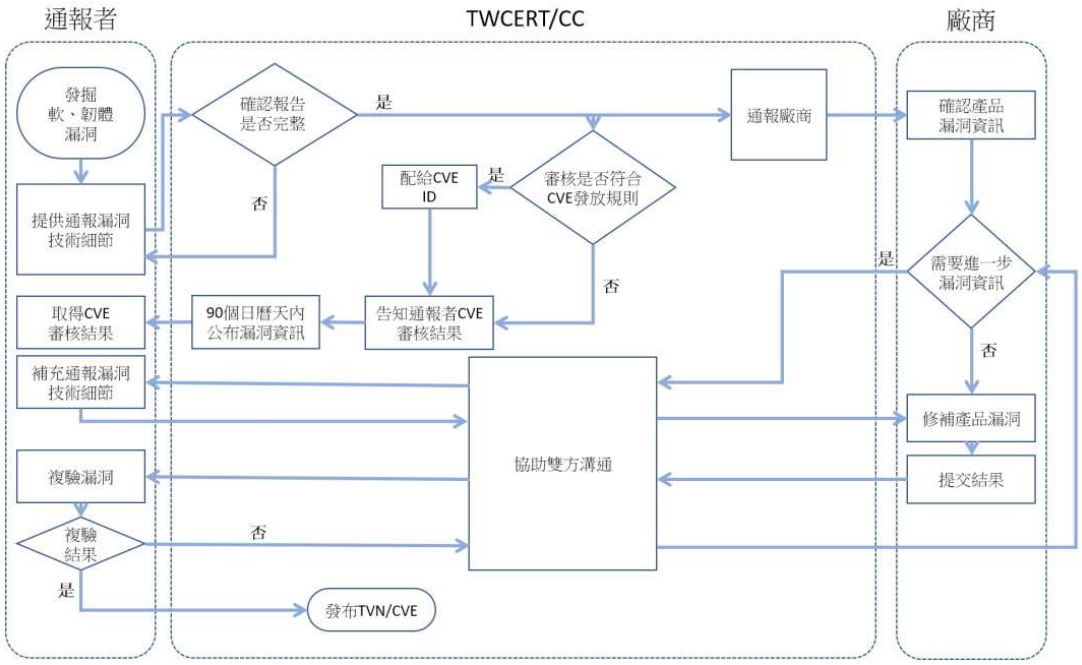
本中心開發台灣漏洞紀錄(Taiwan Vulnerability Note, TVN)平台，將於此平台中提供漏洞通報紀錄，包含公開日期、影響產品、問題描述、解決方法、CVE 編號、相關連結、漏洞通報者等資訊。

3. 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 1 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 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，本中心將把漏洞資訊公布於 TVN 平台中。



資料來源：TWCERT/CC

圖 1 漏洞報告處置流程

4. 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 2 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。

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：

4.1 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。

4.2 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。

4.3 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。

4.4 Rule 4：Requirements for Assigning a CVE ID Rule

4.4.1 Rule4.1：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。

4.4.2 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。

4.4.3 Rule 4.3：漏洞是否為使用者可控制版本的軟體

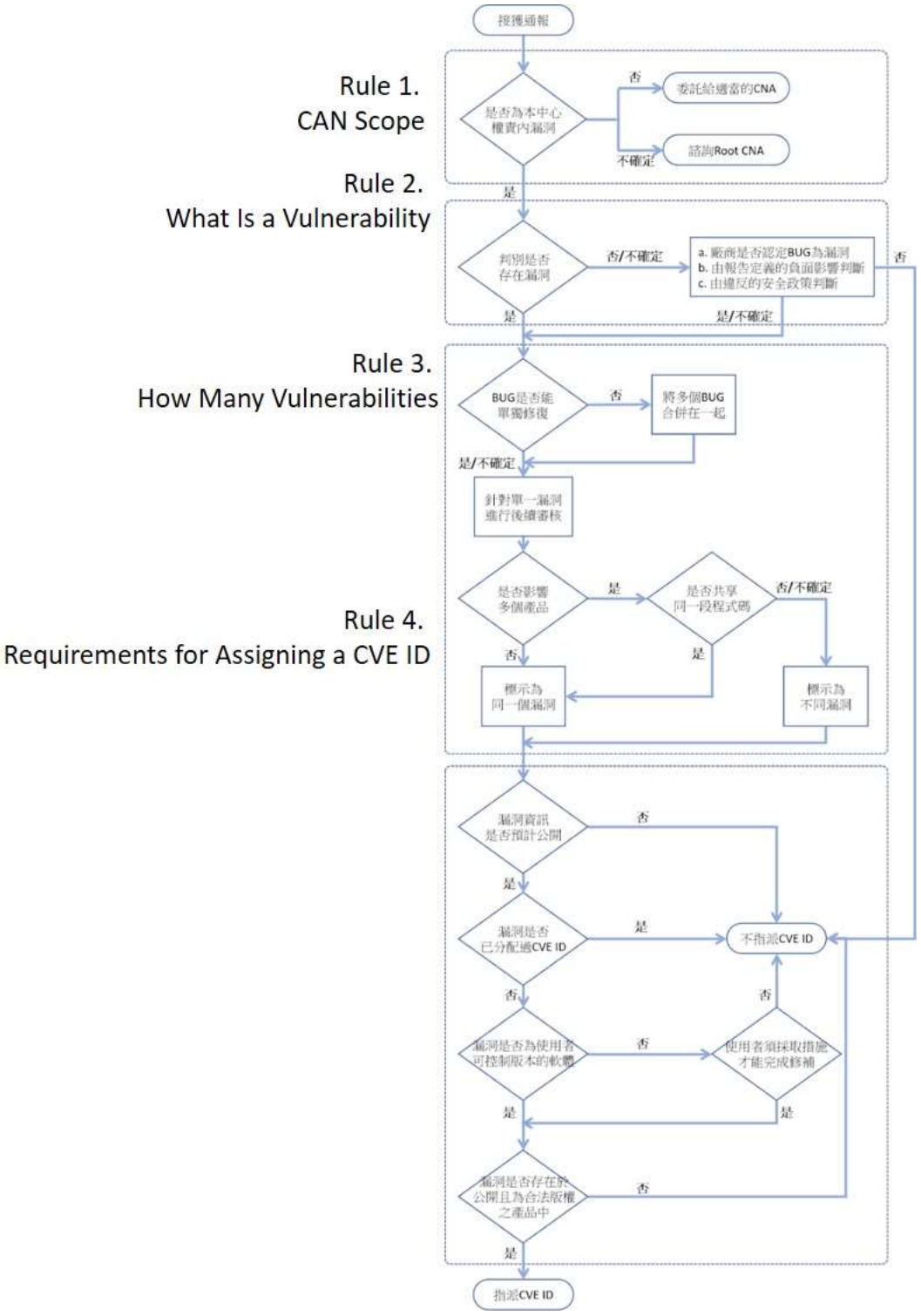
- 若受漏洞影響之產品或服務版本為使用者可控制，則發放 CVE ID。
- 若產品或服務之版本不受使用者控制，但該漏洞需要使用者採取措施才能解決，亦會發放 CVE ID。
- 若使用者無法對有漏洞的產品採取任何緩解措施或修復程序，則無法發放 CVE ID 給該漏洞，如線上網站(例如 Google.com) 及軟體即服務(Software-as-a-Service, SaaS)等，此類產品就算出現漏洞也無法發放 CVE ID。
- 若產品雖為 SaaS，但仍有安裝在少數客戶端上的軟體存在漏洞，則仍會發放此產品該漏洞的 CVE ID；若漏洞同時影響 SaaS 版和客戶端安裝版，亦會發放 CVE ID。

4.4.4 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

CVEID。

- 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。



資料來源：TWCERT/CC

圖 2 CVE 編號發放規則