TWCERT/CC Coordinated Vulnerability Disclosure Policy

Version 2.2

March 18, 2025

Notification

This document is marked TLP: CLEAR, and disclosure is not limited. Sources may use TLP: CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP: CLEAR information may be distributed without restriction.

CONTENT

List of Figures

1. Introduction

Taiwan Computer Emergency Response Team/Coordination Center (TWCERT/CC) is operated by the National Institute of Cyber Security (NICS) under the supervision of the Ministry of Digital Affairs (moda).

To enhance Taiwan's cybersecurity capabilities, TWCERT/CC leads efforts in cybersecurity incident reporting, collaborates with cybersecurity organizations, academic institutions, civil communities, government agencies, private enterprises, and CERTs/CSIRTs worldwide, and integrates resources to strengthen cyber defense.

TWCERT/CC aims to serve as a trusted intermediary. Since 2018, it has been a member of the Common Vulnerabilities and Exposures (CVE®) program[1] as a CVE Numbering Authority (CNA), managed by The MITRE Corporation. Additionally, TWCERT/CC has developed the Taiwan Vulnerability Note (TVN) platform to facilitate vulnerability disclosure, as well as patching and mitigation efforts, thereby preventing the exploitation of vulnerabilities.

All these efforts are aimed at helping enterprises address reported vulnerabilities in their products, thereby enhancing and promoting Taiwan's cybersecurity. The focus is on safety, convenience, and efficiency to foster a secure Internet environment.

2. Bug and Vulnerability Reporting

To report bugs or vulnerabilities you have discovered to TWCERT/CC, please email your report with detailed information and supporting evidence to cve@cert.org.tw. The follow-up process will be initiated after receiving your report.

If you feel the need to encrypt your communications, TWCERT/CC's PGP key (Key ID: 1E9D1F1B) is available at: https://www.twcert.org.tw/tw/cp-26-75-6ad16-1.html.

3. Disclosure Policy

The vulnerability disclosure and handling procedures of TWCERT/CC are based on the CVE Numbering Authority (CNA) Rules[2] published by the official CVE® Program and the laws of the Taiwan.

---

[1] More information about CVE program can be found on their official website: https://cve.mitre.org/

TWCERT/CC handles vulnerabilities in accordance with the CVE Numbering Authorities (CNA) Rules[2] and the laws of Taiwan. In the event of any ambiguity or insufficient clarification within the following provisions, TWCERT/CC reserves the sole and final right of interpretation.

3.1. Definitions

3.1.1. Bug

A bug is defined as a flaw or design oversight that may lead to a potential vulnerability.

3.1.2. Vulnerability

A vulnerability is defined as a weakness in computational logic (e.g., code) found in software or hardware components that, when exploited, can negatively affect confidentiality, integrity, or availability.

3.1.3. Mitigation

Mitigation is defined as the elimination of a vulnerability through code modifications. However, if the vulnerability is addressed by altering or reducing the specifications or functionalities of the software or firmware, such actions are not considered mitigation. For example, directly removing the vulnerable functionality or disabling the affected communication port does not qualify as mitigation.

3.1.4. Reporter

A reporter is defined as a security researcher, a corporate partner, an end user, etc., who submits the details of a discovered product vulnerability, along with relevant supporting evidence, to TWCERT/CC.

3.1.5. Vendor

A vendor is defined as the manufacturer or developer of the product that contains the

2 More information about CVE Numbering Authorities (CNA) Rules can be found on their official website: https://www.cve.org/ResourcesSupport/AllResources/CNARules

vulnerability.

3.1.6. CVE

Common Vulnerabilities and Exposures (CVE) is a list of entries, each containing an identification number, a description, and at least one public reference for publicly known cybersecurity vulnerabilities.

CVE entries are widely used in numerous cybersecurity products and services around the world, including the U.S. National Vulnerability Database (NVD).

3.1.7. CVE ID

Each vulnerability recorded in the CVE database is assigned a unique identifier to facilitate referencing of a specific vulnerability. This identifier is referred to as a CVE ID, and may also be known as a CVE Entry, CVE, or CVE number.The standard format of a CVE ID is “CVE-Year (4 digits)-Serial number (no less than 4 digits).”

3.1.8. CNA

CVE Numbering Authorities (CNAs) are voluntary organizations, which may include national CERTs, industry CERTs, research institutions, vulnerability reporting organizations, or vendors from around the world. Each CNA is authorized to assign CVE IDs to vulnerabilities in products within their distinct, agreed-upon scope and is responsible for maintaining the associated CVE entries.

3.1.9. Shared Codebase

A codebase is defined as a collection of source code that contains various functional modules or components used to build systems, applications, or software products. A shared codebase is defined as a codebase that is utilized across multiple products.

3.2. Disclosure Timeline

Vulnerabilities reported to TWCERT/CC will be disclosed to the public within 90 calendar days from the date the report is confirmed to be complete. The disclosed information includes the title, disclosure date, affected products, a brief description, and the identity of the reporter. TWCERT/CC reserves the right to postpone the disclosure schedule and adjust the level of

detail disclosed, based on an assessment of the vulnerability's potential impact.

3.3. Vulnerability Notes

TWCERT/CC developed Taiwan Vulnerability Note (TVN) platform, which is the website TWCERT/CC discloses the vulnerabilities. The information disclosed on the website including reporting date, detected date, affected product, description, solution, CVE ID, reference, and reporter.

The TVN platform is still under development now. Therefore, before the TVN platform is ready for use, TWCERT/CC will disclose the information when assigning CVE IDs in our official website.

3.4. Vulnerability Handling Process

The vulnerability handling process at TWCERT/CC following the receipt of a vulnerability report is illustrated in Figure 1. When a reporter discovers a vulnerability, they submit the technical details to TWCERT/CC. Upon receiving the report, TWCERT/CC conducts an initial assessment to determine whether the report contains sufficient information. If the report is incomplete, the reporter will be requested to provide additional information. Once the report is deemed complete, a TVN (Taiwan Vulnerability Note) ID will be assigned to the case, and the basic vulnerability information will be disclosed on the TVN platform within 90 calendar days.

Subsequently, the vulnerability report is forwarded to the product vendor for confirmation. TWCERT/CC facilitates communication between the reporter and the vendor, including the verification of vulnerability information and confirmation of remediation results.

Finally, once all parties confirm that the vulnerability has been resolved or that appropriate mitigation measures have been implemented, TWCERT/CC will publicly disclose the vulnerability information on the TVN platform.

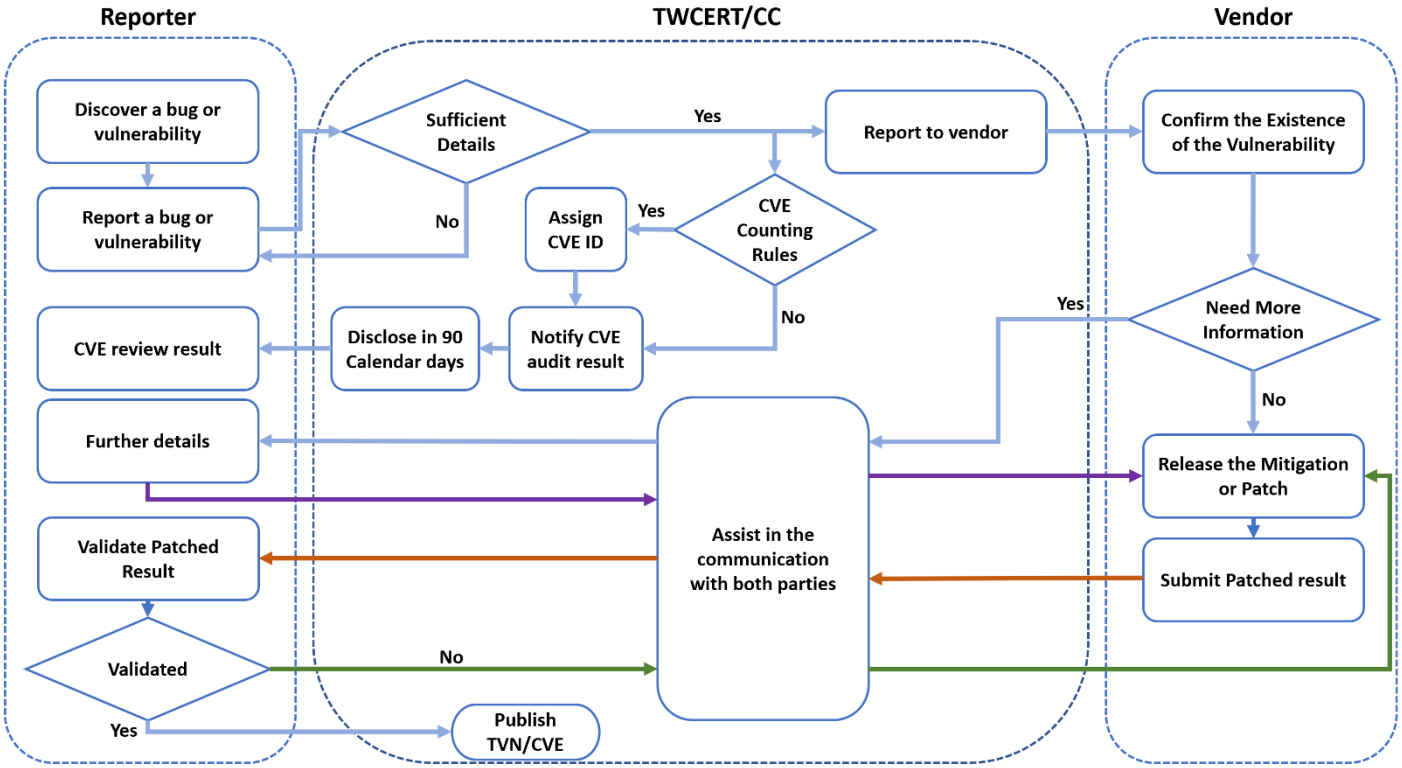

Figure 1 Vulnerability Handling Process

3.5. CVE Counting Rules

If the reporter, TWCERT/CC, or the product vendor wishes to apply for a CVE ID during the vulnerability handling process, TWCERT/CC will take the lead in verifying whether the vulnerability meets the criteria defined in the official CVE Counting Rules, as illustrated in Figure 2. Once the eligibility is confirmed and the product vendor has validated the vulnerability information, TWCERT/CC, as a CNA (CVE Numbering Authority), will assign a CVE ID to the vulnerability.

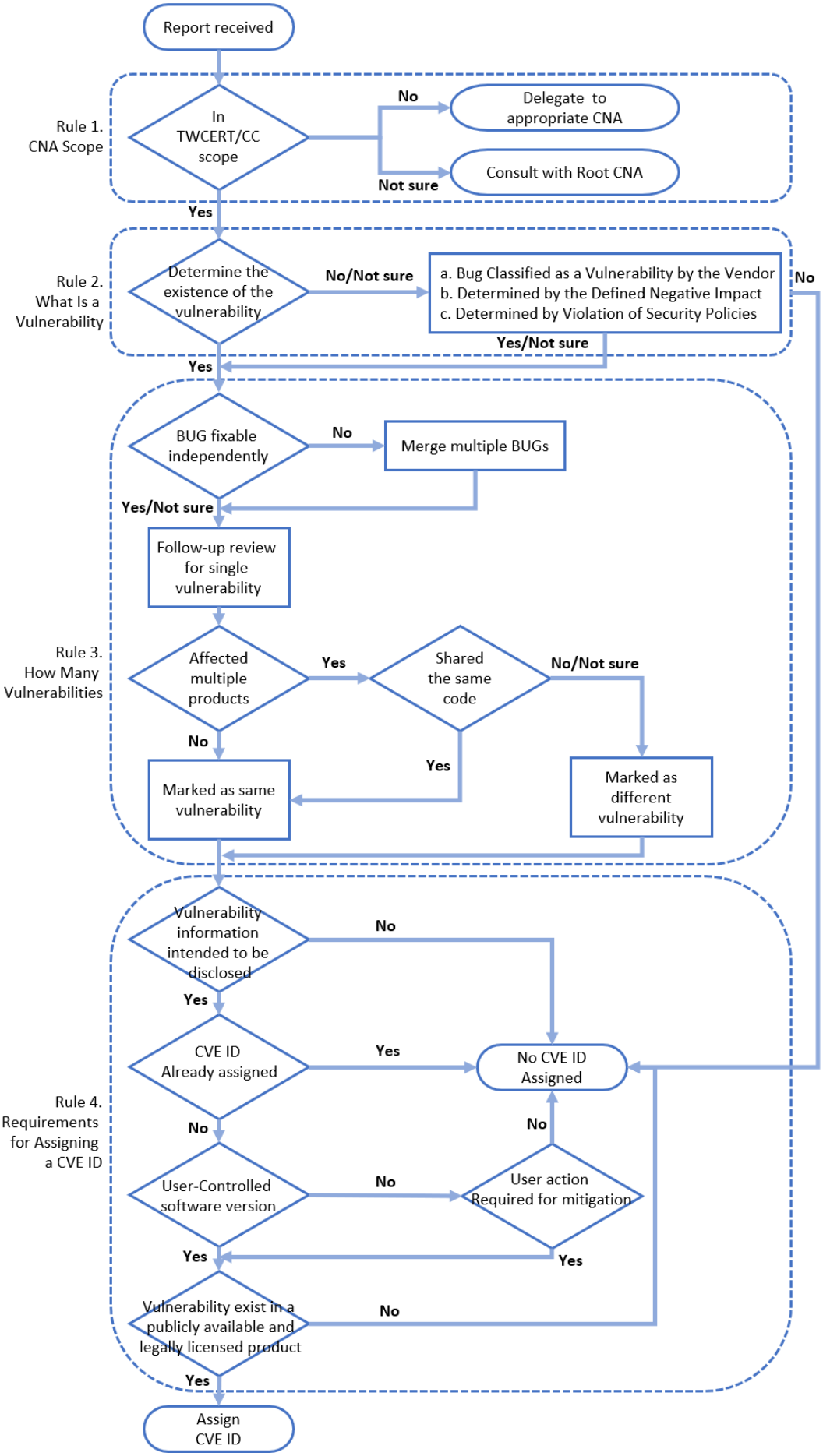

Figure 2 CVE Counting Rules

The CVE ID assignment rules consist of four criteria. Only when all of these criteria are met can it be determined how many distinct vulnerabilities are involved and whether a CVE ID can be assigned to each one. In other words, there may be cases where a CVE ID cannot be assigned to a particular vulnerability. The following provides an overview of each assessment criterion.

3.5.1. Rule 1: CNA Scope

- Since each CNA has a different area of responsibility, it is essential to confirm which CNA's scope the vulnerability falls under before publishing it. The corresponding CNA will be responsible for assigning the CVE ID.
- If no directly responsible subordinate CNA can be identified, the vulnerability may be escalated to the Root CNA.
- A single vulnerability can be jointly handled by multiple CNAs.
- If the vulnerability falls within the scope of multiple CNAs, the Root CNA is responsible for coordinating the handling process.
- If it is unclear which CNA's scope the vulnerability falls under, the Root CNA may be consulted for clarification.

3.5.2. Rule 2: What Is a Vulnerability

- Identify the product manufacturer of the product that contains the bug and determine whether the bug qualifies as a vulnerability.
- The product manufacturer must confirm whether the bug constitutes a vulnerability that could have a negative impact on the product.
- If the product manufacturer is unwilling or unable to confirm whether the bug is a vulnerability, or is unwilling to support patching the identified vulnerability, the determination can be made based on the vulnerability reporter's assessment or whether the bug violates the product manufacturer's security policy.

3.5.3. Rule3: How Many Vulnerabilities

- Each bug must be able to be fixed independently, without requiring the resolution of other bugs.
- If fixing Bug A also resolves Bug B, then Bug A and Bug B should be merged and treated as Bug A. If it is unclear whether one or multiple bugs can be fixed

independently, they should be treated as a single bug.

For reviewing a single vulnerability:

- If the vulnerability affects only a single product, it should be labeled as the same vulnerability.
- If the same code is shared across multiple products, the vulnerability should be labeled as the same for those products.
- If multiple products are affected but use different code, the vulnerability should be labeled as a different vulnerability for each product. If this cannot be determined or is undefined, treat each product as having a different vulnerability.

If the vulnerability arises from the use of a vulnerable library, protocol, or standard:

- If the vulnerability is caused by a library used by the product due to compliance with a specific specification, it should be labeled as the same vulnerability for that library, protocol, or standard.
- If the vulnerability is caused by the implementation of the library, protocol, or standard, it should be labeled as the same vulnerability for each affected library.
- If the cause is uncertain, label it as a different vulnerability for each affected library.

3.5.4. Rule 4: Requirements for Assigning a CVE ID

Rule 4.1: Vulnerability information intended to be disclosed

- In order to assign a CVE ID to a vulnerability, the basic information of the vulnerability must be publicly available through an accessible URL. The basic information must include the product name, version, and issue type (i.e., vulnerability type or impact).
- It is acceptable if the information at the URL is accessible for free after registration and login, but no additional restrictions should apply. If more detailed technical information requires a paid subscription, the vulnerability can still be considered publicly disclosed.

Rule 4.2: Ensure No Duplicate Vulnerability Exists in CVE

- Check the official CVE list (URL: https://cve.mitre.org/index.html) to verify whether the vulnerability has already been assigned a CVE ID. If a CVE ID already exists, a new one will not be issued.

Rule 4.3: Whether the vulnerability is in a user-controlled version of the software

- If the affected product or service version is user-controlled, a CVE ID will be assigned.
- If the product or service version is not user-controlled but the vulnerability requires

user action to resolve, a CVE ID will still be assigned.

- If users cannot take any mitigation or remediation actions on a vulnerable product, a CVE ID will not be assigned. This applies to cases such as websites (e.g., Google.com) or Software-as-a-Service (SaaS) offerings. Even if a vulnerability exists, no CVE ID will be assigned in such scenarios.
- If a product is SaaS-based but also includes software installed on a limited number of client systems, a CVE ID will still be assigned for the vulnerability. If the vulnerability affects both the SaaS version and the client-installed version, a CVE ID will be issued.

Rule 4.4: Whether the vulnerability exists in a publicly available and legally licensed product

- If the vulnerability exists in an unpublished or unauthorized product, a CVE ID will not be assigned.
- Only vulnerabilities in publicly accessible products with legal licensing are eligible for CVE ID assignment. Vulnerabilities found in software used exclusively within a single organization or in malware are not eligible for a CVE ID.
- Vulnerabilities in non-final products—such as discontinued beta versions or pre-release patch versions submitted before the official release—are not eligible for CVE ID assignment.

3.6. Disclosure of Reporter's Name and Contact Information

To ensure proper credit, the reporter’s name will be disclosed on the TVN platform along with the vulnerability report. The name may include, but is not limited to, a nickname or an organization name. If the reporter does not wish to disclose their name, they may request anonymity at any time. TWCERT/CC will then assist in modifying the record to display the reporter as anonymous.

As a coordinator, TWCERT/CC facilitates communication between the reporter and the vendor, assisting both parties with verifying vulnerability details and tracking remediation progress. If the vendor requires additional information regarding the reported vulnerability, TWCERT/CC will first ask the reporter whether they consent to sharing their contact information (such as phone number or email) with the vendor. If the reporter agrees, the vendor may directly contact the reporter to clarify vulnerability details. However, the vendor is still required to update TWCERT/CC on the remediation status to ensure the vulnerability report remains up to date. If the reporter does not consent, the vendor will not be given direct contact

information, and TWCERT/CC will act as an intermediary for communication between both parties.

4. Contact TWCERT/CC

- Official website: https://www.twcert.org.tw/
- E-mail: twcert@cert.org.tw
- Report a vulnerability: cve@cert.org.tw
- Report an incident: https://www.twcert.org.tw/en/cp-57-96-6ca30-2.html

5. References

[1] Common Vulnerabilities and Exposures, https://cve.mitre.org/

[2] CVE Numbering Authority (CNA) Operational Rules , https://www.cve.org/resourcessupport/allresources/cnarules

[3] CERT/CC Vulnerability Disclosure Policy. “CERT® Guide to Coordinated Vulnerability Disclosure”, https://vuls.cert.org/confluence/display/Wiki/Vulnerability+Disclosure+Policy