TLP:WHITE

TWCERT/CC Vulnerability Disclosure and Coordination Policy

Version 1.4

October 11, 2018

Notification

This document is marked TLP: WHITE, and disclosure is not limited. Sources may use TLP: WHITE 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: WHITE information may be distributed without restriction.

台灣電腦網路危機處理暨協調中心

Taiwan Computer Emergency Response Team/Coordination Center

CONTENT

List of Figures

1. Introduction

Taiwan Computer Emergency Response Team/Coordination Center (TWCERT/CC) is operated by the National Chung-Shan Institute of Science and Technology (NCSIST) under the supervision of the Executive Yuan.

To enhance Taiwan's cyber security capacity, TWCERT/CC leads the promotion of cyber security incident reporting, collaborates and integrates resources with cyber security organizations, academic institutions, civil communities, governmental institutions, private enterprises, and CERTs/CSIRTs all over the world.

TWCERT/CC aims to work as a trusted intermediary. Therefore, since 2018 TWCERT/CC is a member with the CVE Numbering Authority (CNA) status of the Common Vulnerabilities and Exposures (CVE®) program[1] maintained by The MITRE Corporation. Moreover, TWCERT/CC has developed the Taiwan Vulnerability Note (TVN) platform to facilitate the disclosure of vulnerabilities and further patchings and mitigations hence to prevent the exploitation of vulnerabilities.

All the aforementioned duties and efforts are to help enterprises to deal with the reported vulnerabilities in their products therefore to protect and promote Taiwan's cyber security with emphases on safety, convenience, and efficiency hence to develop a secure Internet environment.

2. Bug and Vulnerability Reporting

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

If you feel the need to encrypt your communications with TWCERT/CC's PGP key (KeyID: 1E9D1F1B), it is available from: https://twcert.org.tw/subpages/aboutus/pgp_key.aspx.

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

3. Disclosure Policy

TWCERT/CC handle vulnerabilities in accordance with the CVE Numbering Authorities (CNA) Rules[2] and the laws of Taiwan. In case of any dispute, TWCERT/CC has sole and final discretion of interpretation of these Terms and Conditions.

3.1. Definitions

3.1.1. Bug

A bug is the flaw or design oversight leading to a potential vulnerability.

3.1.2. Vulnerability

Vulnerability is defined as a weakness in the computational logic (e.g., code) found in software and hardware components that, when exploited, results in a negative impact to confidentiality, integrity, OR availability.

3.1.3. Mitigation

Mitigation of the vulnerabilities in this context typically involves coding changes, but could also include specification changes or even specification deprecations (e.g., removal of affected protocols or functionality in their entirety).

3.1.4. Reporter

The one who is including but not limited to a person/organization/researcher, and reports the bugs or vulnerabilities to TWCERT/CC.

3.1.5. Vendor

The developer or producer of the vulnerable products.

3.1.6. CVE

CVE (Common Vulnerabilities and Exposures, CVE) is a list of

2 More information about CVE Numbering Authorities (CNA) Rules can be found on their official website: https://cve.mitre.org/cve/cna/rules.html

entries—each containing an identification number, a description, and at least one public reference—for publicly known cybersecurity vulnerabilities.

CVE Entries are used in numerous cybersecurity products and services from around the world, including the U.S. National Vulnerability Database (NVD). [1]

3.1.7. CVE ID

CVE ID is also known as "CVE Entry," "CVE," and "CVE number", provide reference points for data exchange so that cybersecurity products and services can speak with each other.

The format of CVE ID is “CVE prefix-year (4 digits)-serial number (no less than 4 digits).” For example, the CVE ID of the vulnerability used in WannaCry ransomware is CVE-2017-0144.

3.1.8. CNA

CVE Numbering Authorities (CNAs) are organizations that are authorized to assign CVE IDs to vulnerabilities affecting products within their distinct, agreed upon scope, for inclusion in first-time public announcements of new vulnerabilities.

Participation in this program is voluntary, and the benefits of participation include the ability to publicly disclose a vulnerability with an already assigned CVE ID, the ability to control the disclosure of vulnerability information without pre-publishing, and notification of vulnerabilities in products within a CNA’s scope by researchers who request a CVE ID from them.

CNAs are categorized as Primary, Root, and Sub-CNAs (or just “CNAs”, generically). Multiple Sub-CNAs may operate under the oversight of a Root CNA, while the Root CNAs operate under the oversight of a single, Primary CNA or another Root CNA. Sub-CNAs only assign CVEs for vulnerabilities in their own products or their domain of responsibility, hereinafter referred to as scope. Root CNAs manage a group of Sub-CNAs within a given domain or community, train and admit new Sub-CNAs, and are the assigners of last resort (i.e., no Sub-CNA exists for the scope) within that domain or community. The Primary CNA oversees the CVE Program, coordinates Root CNAs and Sub-CNAs, trains and admits new

Root CNAs and Sub-CNAs, enables Root CNAs to administer their CVE scope, and is the assigner of last resort for requesters that are unable to have CVEs assigned at the Sub- or Root CNA levels. [2]

3.1.9. Shared Codebase

A codebase is a software component that is shared among multiple products. [2] A shared codebase is a codebase which was used in multiple products.

3.2. Disclosure Timeline

Vulnerabilities reported to the CERT/CC will be disclosed to the public in 45 calendar days after the initial report. Disclosed information includes title, reporting date, detected date, affected product, brief description, and reporter. For instance, if we received a report on August 1st, 2018, we will disclose the information mentioned above no later than September 14th, 2018.

Detailed description, technical detail and solution of the report will be disclosed only if the mitigation or patch of the vulnerability is avaliable, or the vulnerability has been confirmed as harmless. There is no time limit of the disclosure of the information mentioned above.

By evaluating the potential impact caused by the reported vulnerability, we have the right to postpone the disclosure time of any information related to the vulnerability.

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].

[3] English version: https://twcert.org.tw/subpages/ServeThePublic/public_document.aspx?lang=en-US; Chinese version: https://twcert.org.tw/subpages/ServeThePublic/public_document.aspx

3.4. Vulnerability Handling Process

After a reporter discovered a bug or vulnerability, he/she can report it with detailed information to us.

Firstly, we will ensure if the information in the report is sufficient or not. If so, we will generate a unique TVN number for the report, and disclose essencial information on TVN platform in 45 calendar days. Otherwise, we will return the report to the reporter and ask for further infomarion.

Secondly, we will provide the report to affected vendor for confirming the existence of the vulenrability. As a coodinator, we will assis in the communication with both reporter and vendor, and help both parties to deliver message and validate the patch of vulnerability.

Finally, after the mitigation or patch of the vulnerability is released, we will disclose detailed information on TVN platform.

However, we will regard the report as invaid if any of the following situation happened:

- The information provided is not sufficient enough to define the vulnerability.
- Against CVE Numbering Authorities (CNA) Rules. [2]
- Unable to contact the reporter for further information.

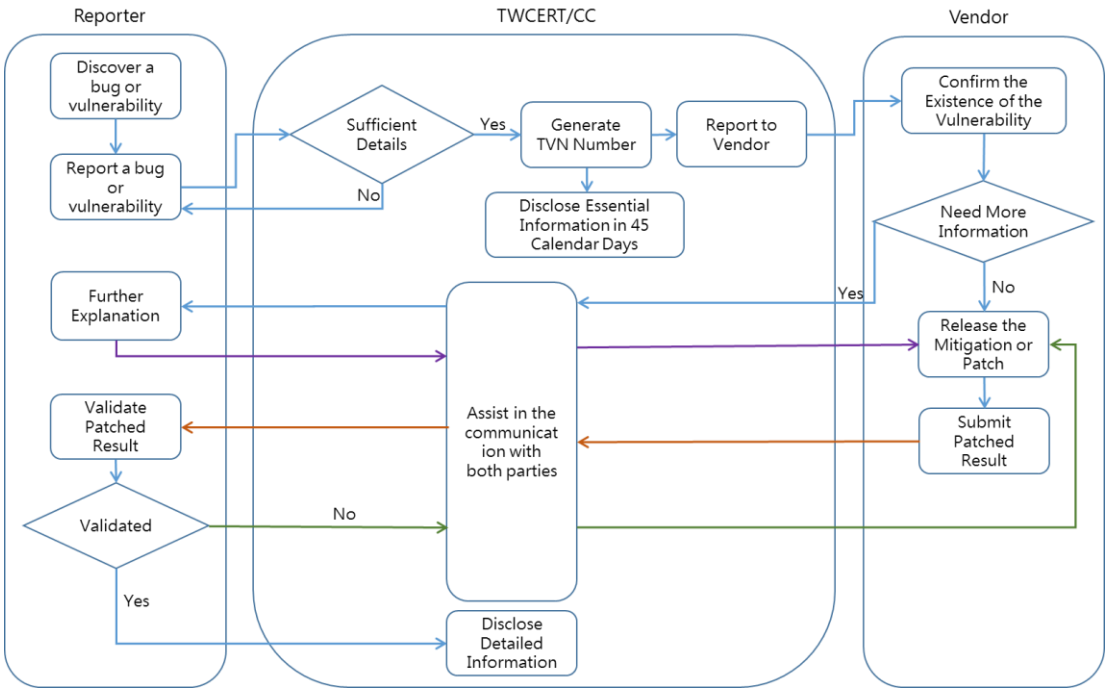

Figure 1 Vulnerability Handling Process

3.5. CVE Counting Rules

Once us, reporter or vendor wish to apply a CVE ID for the vulnerability through vulnerability handling process, we will coordinate three parties to work together and confirm if the vulnerability meets the needs in CVE Counting Rules (Figure 2) or not. If so, as a CNA, we will assign a CVE ID for the vulnerability.

CVE Counting Rules include Counting (CNT) decisions and Inclusion (INC) decisions parts. CNT decisions can be used to determine how many vulnerabilities there are in a report. On the other hand, INC decisions can be used to to determine if a vulnerability should be assigned a CVE ID or not.

Comprehensive CVE Counting Rules can be found in the link below: https://cve.mitre.org/cve/cna/rules.html#Appendix_C

3.6. Disclosure of Reporter's Name and Contact Information

To give the credit, the name of the reporter will be disclosed with the report on TVN platform. The reporter could request to be

anonymous anytime if he/she doesn’t want the name to be disclosed.

As a coodinator, we will provide essential assistance, and assist both reporter and vendor to communicate with each other. If the vendor wants to ask for further detail about the reported vulnerability, we will ensure if the reporter allows the name and contact information to be provided to the vendor. If so, the reporter’s contact information will be provided to the vendor, and the vendor can contact the reporter directly. Otherwise, we will act as a bridge between reporter and vendor.

4. Contact TWCERT/CC

- Official website:

  https://www.twcert.org.tw/

- Phone:

  +886-2-23776418 (Taipei Office)

  +886-3-4115579 (Taoyuan Office)

- E-mail:

  twcert@cert.org.tw

- Report a vulnerability:

  cve@cert.org.tw

- Report an incident:

  http://surl.twcert.org.tw/mvPLG

5. References

[1] Common Vulnerabilities and Exposures. ”Common Vulnerabilities and Exposures”, Retrieved August 17th, 2018, from the World Wide Web:
https://cve.mitre.org/

[2] CVE Numbering Authorities (CNA) Rules, “CVE Numbering Authorities (CNA) Rules”, Retrieved August 17th, 2018, from the World Wide Web:
https://cve.mitre.org/cve/cna/rules.html

[3] CERT Vulnerability Disclosure Policy, “Vulnerability Disclosure Policy”, Retrieved August 17th, 2018, from the World Wide Web:
https://vuls.cert.org/confluence/display/Wiki/Vulnerability+Disclosure+Policy