Common Vulnerabilities and Exposures

CVE IDs and How to Get Them

Daniel Adinolfi

Anthony Singleton

The MITRE Corporation

Agenda

- CVE Overview
- How to Get CVE IDs
- Getting your CVE ID published
- Updating CVE IDs and Working with CVE
- Questions and Wrap-up

CVE Description, Purpose, and Value

- **CVE is a dictionary of publicly known cybersecurity vulnerabilities**
- **Purpose: To uniquely identify and name publicly disclosed vulnerabilities pertaining to specific versions of software or codebases**
- **Value: Stakeholders have confidence that they can refer to a CVE Identifier (ID) and know they are talking about a specific, unique vulnerability regardless of the tool or forum being used**

What CVE Is and Is Not

CVE is…

- **The de facto standard for uniquely identifying vulnerabilities**
- **A dictionary of publicly known cybersecurity vulnerabilities**
- **A pivot point between vulnerability scanners, vendor patch information, patch managers, and network/cyber operations**

CVE is not…

- **A vulnerability mitigation**
  - CVE IDs uniquely define vulnerabilities so that mitigations can be efficiently applied
- **A vulnerability database**
  - CVE allows vulnerability databases to be linked together under commonly used IDs
- **A source for vulnerability risk, impact, fix, or technical information**
  - Each CVE contains a unique ID, description, and references
- **A tool for publicly disclosing vulnerabilities**
  - CVE uses publicly disclosed vulnerability information as its source of information

Who Can Assign CVE IDs?

- **The MITRE Corporation**
  - Oversees the CVE Program operationally and administratively
- **CVE Numbering Authorities**
  - CNAs are organizations that assign CVE IDs to researchers and vendors for inclusion in first-time public announcements of new vulnerabilities
  - Each CNA has a specific scope of responsibility, delimiting what products, information sources, or domains for which they assign CVEs
  - Includes Vendor PSIRTs, National CERTs, Researchers, and Bug Bounties

When Can You Request a CVE ID?

1. **You have identified a new or previously unassigned vulnerability in any product. (You don't need to have discovered it.)**
2. **You have attempted to contact the vendor/developer of the affected product.**
   - If the vendor is a CNA: they will assign the CVE ID for you.
   - If the vendor is not a CNA: to verify whether the issue has already been reported or if another CVE ID has already been assigned for the issue. (It is also the right thing to do.)

- **If you are working with a Coordination Center (like CERT/CC), they will direct you to contact CVE at the right time.**

- **The vulnerability does not have to be public before you request a CVE ID, but it does need to be public to be included in the CVE List.**

Counting

- **Counting is the method used by CVE to determine**
  - If a bug is a vulnerability, and
  - If it is a vulnerability, how many vulnerabilities there actually are.

Counting Process Summary
Determine Number of Vulnerabilities

- **Start by breaking the report into individual bugs**
- **Determine if the individual bugs result in vulnerabilities**
  - For those that do, go to the next step
  - For the bugs that don't, determine if a combination of the bugs results in a vulnerability
- **For the vulnerabilities identified this way, any that are the result of shared code, a protocol, or a standard should be merged into one**
- **Now you know how many. Do they warrant a CVE ID?**

Counting Process Summary
Should a CVE ID Be Assigned?

- **You then determine if there is value to the community in assigning a CVE ID**
  - The information about the vulnerability must be public (If no one knows which vulnerability the ID is assigned to, it doesn't help them.)
  - The community must be able to do something to mitigate the vulnerability
  - The community has to be concerned about the security of the product. (Yes, it is subjective.)
- **Finally, determine if a CVE ID has already been assigned to the vulnerability. If not...**
- **You are ready to request an assignment! (Yay!)**

How to Request a CVE ID

- **Visit https://cveform.mitre.org/ and "Request a CVE ID"**
- **You will need to provide the following at a minimum:**
  - Vulnerability Type
  - Vendor or developer of the product or project
  - The affected product/project and version information.
- **You may provide the following optionally:**
  - Attack type
  - Impact
  - Affected component
  - Attack vector(s)
  - If the vendor/developer has acknowledged the vulnerability
  - Public references

What Happens Next?

- **You will receive a confirmation email message. (Keep this. It's lovely.)**
- **MITRE will review the request.**
  - If there is sufficient information to indicate that the assignment is valid, the Content Team will send you the CVE ID to use.
  - If the vulnerability is in a product covered by a CNA, Content Team will direct you to the appropriate CNA.
  - If there is not enough information to indicate that the assignment is valid, the Content Team will ask the requester for more info.
- **If a CVE ID is assigned to the vulnerability, it will be marked as "RESERVED" in the CVE List.**
- **At this point, the CVE ID entry does not contain any vulnerability details. The details will not be published in the CVE List until...**

Populating a New CVE ID

- **A CVE ID must reference public information. Public references must be included in a CVE ID entry before it is published.**
  - If you requested a CVE ID and have created a public reference including the details about the vulnerability, **NOTIFY MITRE (or the CNA)** and include the reference information.
  - You may keep an assigned CVE ID without publishing it if you are under an embargo, but when the embargo ends, you should **UPDATE MITRE**.
- **Once the CVE ID has a public reference and MITRE (or the CNA) has been notified that the vulnerability is public, MITRE will populate the CVE entry description and fully-publish the CVE ID.**
- **Gratz! You have a fully-published CVE ID.**

Description Writing

- We encourage the community to provide CVE entry descriptions when they request a CVE ID
- CVE entry descriptions follow a set of requirements and formatting guidelines

How to Write a Description

- **Must contain the product, version, and problem type information**
  - The product, version, and problem type are also submitted as separate field
  - They need to be in both locations because the separate fields are not currently included in the CVE List used by downstream users
- **Only information in the provided references can be included in the description**
  - The CVE program needs to be trusted not to leak the privileged information reporters share with it. Requiring that every detail be backed up by another source helps keep this trust.
- **Only relevant information about the vulnerability should be included**
- **Must be in English (when sent to the Primary CNA)**

How MITRE Writes Descriptions

- **If you don't already have a style that works for CVE entries, you can borrow MITRE's template format**
  - **[VULNTYPE]** in **[COMPONENT]** in **[VENDOR][PRODUCT] [VERSION]** allows **[ATTACKER]** to **[IMPACT]** via **[VECTOR]**.
  - **[COMPONENT]** in **[VENDOR] [PRODUCT] [VERSION] [ROOT CAUSE]**, which allows **[ATTACKER]** to **[IMPACT]** via **[VECTOR]**.
- **For more information on MITRE's style see our GitHub site**
  - http://cveproject.github.io/docs/content/key-details-phrasing.pdf

Updating Existing CVE IDs

- **If you have additional information to add to a CVE entry, you may request that the entry be updated with additional information**
- **You can update**
  - References
  - The description
  - Suggest that a CVE ID is a duplicate or should be split into multiple IDs
  - You can dispute whether a CVE ID is valid or not

A Word on Credit and Attribution

- **The CVE List does not include credit or attribution for who discovered or contributed to the discovery of the vulnerability as part of the information it provides**
- **Credit and attribution may be included in the references**
- **CVE is more interested in the community benefitting from the public disclosure of vulnerabilities than from individuals gaining recognition. (Sorry, not sorry.)**

It Takes a Community

- **MITRE wants CVE to be a resource that anyone in any industry in any country can use**
- **You can help**
  - If you find a new vulnerability, SUBMIT IT and give us the information we need to populate the entry!
  - If you have information relevant to a CVE ID that isn't included in its entry, SUBMIT IT!
  - If you are experiencing problems working with a CNA, REPORT IT!
  - If you see an error in a CVE ID, REPORT IT!
  - Do research in medical security? IoT security? Automotive security? You can get CVE IDs for vulnerabilities you discover!
  - Work for a company that cares about vulnerability management? Become a CNA!

Resources

- **CVE Website**
  - http://cve.mitre.org/
- **CNA rules (if you would like to understand the rules)**
  - http://cve.mitre.org/cve/cna/CNA_Rules_v1.1.pdf
- **CVE Webform**
  - https://cveform.mitre.org/
- **CVE ID Request Guidelines**
  - http://cve.mitre.org/cve/researcher_reservation_guidelines
- **CVE Phrasing Documentation.**
  - http://cveproject.github.io/docs/content/key-details-phrasing.pdf

Questions?