Common Vulnerabilities and Exposures

From Wikipedia, the free encyclopedia

The **Common Vulnerabilities and Exposures** (**CVE**) system provides a reference-method for publicly known information-security vulnerabilities and exposures. MITRE Corporation maintains the system, with funding from the National Cyber Security Division of the United States Department of Homeland Security.[1] CVE is used by the Security Content Automation Protocol, and CVE IDs are listed on MITRE's system[2] as well as the US National Vulnerability Database.

CVE identifiers

MITRE Corporation's documentation defines CVE Identifiers (also called "CVE names", "CVE numbers", "CVE-IDs", and "CVEs") as unique, common identifiers for publicly known information-security vulnerabilities in publicly released software packages. Historically, CVE identifiers had a status of "candidate" ("CAN-") and could then be promoted to entries ("CVE-"), however this practice was ended some time ago and all identifiers are now assigned as CVEs (the collective noun for which is an "infestation" of CVEs). The assignment of a CVE number is not a guarantee that it will become an official CVE entry (e.g. a CVE may be improperly assigned to an issue which is not a security vulnerability, or which duplicates an existing entry). CVEs are assigned by a CVE Numbering Authority (CNA); there are three primary types of CVE number assignments:

1. The MITRE Corporation functions as Editor and Primary CNA
2. Various CNAs assign CVE entries for their own products (e.g. Microsoft, Oracle, HP, Red Hat, etc.)
3. Red Hat also provides CVE numbers for open source projects that are not a CNA

When investigating a vulnerability or potential vulnerability it helps to acquire a CVE number early on. CVE numbers may not appear in the MITRE or NVD CVE databases for some time (days, weeks, months or potentially years) due to issues that are embargoed (the CVE number has been assigned but the issue has not been made public), or in cases where the entry is not researched and written up by MITRE due to resource issues. The benefit of early CVE candidacy is that all future correspondence can refer to the CVE number. Information on getting CVE identifiers for issues with open source projects is available from Red Hat.[3]

CVEs are for software that has been publicly released; this can include betas and other pre-release versions if they are widely used. Commercial software is included in the "publicly released" category, however custom-built software that is not distributed would generally not be given a CVE. Additionally services (e.g. a Web-based email provider) are not assigned CVEs for vulnerabilities found in the service (e.g. an XSS vulnerability) unless the issue exists in an underlying software product that is publicly distributed.

CVE data fields

There are several fields within the CVE database.

CVE-ID

This is the actual CVE identifier.

Description

This is a standardized text description of the issue(s). One common entry is:

```
** RESERVED ** This candidate has been reserved by an organization
or individual that will use it when announcing a new security problem.
When the candidate has been publicized, the details for this
candidate will be provided.
```

This means that the entry number has been reserved by Mitre for an issue or a CNA has reserved the number. So in the case where a CNA requests a block of CVE numbers in advance (e.g. Red Hat currently requests CVEs in blocks of 500), the CVE number will be marked as reserved even though the CVE itself may not be assigned by the CNA for some time. Until the CVE is assigned AND Mitre is made aware of it (e.g. the embargo passes and the issue is made public), AND Mitre has researched the issue and written a description of it, entries will show up as "** RESERVED **".

References

This is a list of URLs and other information (such as vendor advisory numbers) for this issue.

Date Entry Created

This is the date the entry was created. For CVEs assigned directly by Mitre, this is the date Mitre created the CVE entry. For CVEs assigned by CNAs (e.g. Microsoft, Oracle, HP, Red Hat, etc.) this is also the date the entry was create by Mitre, not by the CNA. So in the case where a CNA requests a block of CVE numbers in advance (e.g. Red Hat currently requests CVEs in blocks of 500) the entry date would be when that CVE is assigned to the CNA. The CVE itself may not be used for days, weeks, months or even possibly years (e.g. Red Hat maintains blocks of CVEs for older security issues in Open Source software that were not assigned CVEs yet).

Phase (legacy)

The phase the CVE is in (e.g. CAN, CVE); this is no longer used.

Votes (legacy)

Previously board members would vote yea or nay on whether or not the CAN should be accepted and turned into a CVE; this is no longer used.

Comments (legacy)

Comments on the issue, this is no longer used.

Proposed (legacy)

When the issue was first proposed, this is no longer used.

CVE SPLIT and MERGE

CVE attempts to assign one CVE per security issue, however in many cases this would lead to an extremely large number of CVEs (e.g. where several dozen cross-site scripting vulnerabilities are found in a PHP application due to lack of use of htmlspecialchars() or the insecure creation of files in /tmp). To deal with this there are guidelines (subject to change) that cover the splitting and merging of issues into distinct CVE numbers. As a general guideline consider issues to be merged, then split them by the type of vulnerability (e.g. buffer overflow vs. stack overflow), then by the software version affected (e.g. if one issue affects version 1.3.4 through 2.5.4 and the other affects 1.3.4 through 2.5.8 they would be SPLIT) and then by the reporter of the issue (e.g. Alice reports one issue and Bob reports another issue the issues would be SPLIT into separate CVE numbers). Another example is Alice reports a /tmp file creation vulnerability in version 1.2.3 and earlier of ExampleSoft web browser, in addition to this issue several other /tmp file creation issues are found, in some cases this may be considered as two reporters (and thus SPLIT into two separate CVEs, or if Alice works for ExampleSoft and an ExampleSoft internal team finds the rest it may be MERGE'ed into a single CVE). Conversely issues can be merged, e.g. if Bob finds 145 XSS vulnerabilities in ExamplePlugin for ExampleFrameWork regardless of the versions affected and so on they may be merged into a single CVE.[4]

Search CVE identifiers

The Mitre CVE database can be searched at the CVE List Master Copy (https://cve.mitre.org/cve/cve.html), and the NVD CVE database can be searched at Search CVE and CCE Vulnerability Database (https://web.nvd.nist.gov/view/vuln/search).

See also

- CVSS

References

1. ^ "CVE – Common Vulnerabilities and Exposures" (https://cve.mitre.org/). MITRE Corporation. 3 July 2007. Retrieved 2009-06-18. "CVE is sponsored by the National Cyber Security Division of the U.S. Department of Homeland Security."
2. ^ CVE.MITRE.org (https://CVE.MITRE.org). CVE® International in scope and free for public use, CVE is a dictionary of publicly known information security vulnerabilities and exposures.
3. ^ "CVE OpenSource Request HOWTO" (https://people.redhat.com/kseifrie/CVE-OpenSource-Request-HOWTO.html). Red Hat Inc. 18 June 2012. Retrieved 2013-07-06. "There are several ways to make a request depending on what your requirements are:"
4. ^ CVE Abstraction Content Decisions: Rationale and Application (https://cve.mitre.org/cve/editorial_policies/cd_abstraction.html)

External links

- Official website (https://cve.mitre.org/)
- National Vulnerability Database (https://nvd.nist.gov/)
- vFeed the Correlated and Aggregated Vulnerability Database- SQLite Database and Python API (https://github.com/toolswatch/vFeed)

- CVE Details - Third party CVE database web site (http://cvedetails.com/)
- CVE OpenSource Request HOWTO (https://people.redhat.com/kseifrie/CVE-OpenSource-Request-HOWTO.html)
- CCE (https://nvd.nist.gov/cce/index.cfm)

Categories: Computer security | Computer security exploits | Mitre Corporation

---