CVE Blog

Read more posts on CVE Website or Medium.

All CVE Blog articles published in calendar year 2017 are included in this single PDF.

Table of Contents:

- **CNA Rules, Version 2.0 to Take Effect on January 1st**, October 13, 2017
- **Become a CNA**, August 2, 2017
- **Come Meet with *CVE at Black Hat 2017* on July 27 and *DEF CON 25* on July 28**, July 20, 2017
- **Marking a CVE ID "REJECT" Is Not Permanent; It Can Be Updated and Added to the CVE List**, June 27, 2017
- **Why Is a CVE Entry Marked as "RESERVED" When a CVE ID Is Being Publicly Used?**, May 10, 2017
- **The Significance and Meaning of a CVE Identifier Marked as "RESERVED"**, March 16, 2017
- **Summary of Your Feedback About Updating Info in CVE ID Descriptions**, February 2, 2017
- **The Significance and Meaning of the Year Portion of a CVE Identifier**, January 17, 2017

CNA Rules, Version 2.0 to Take Effect on January 1st

CVE Blog | October 13, 2017

The policies and processes managing the CVE Numbering Authorities (CNAs) Program, known as the "CNA Rules," have been revised with significant input from the CNA community. These revised rules, *CVE Numbering Authorities (CNA) Rules, Version 2.0*, will go into effect on **January 1, 2018**.

CNA Rules, Version 2.0, which is updated from Version 1.1, includes the following clarifications and improvements:

- Fixed a number of typos and reworded some phrasing for clarity.
- Clarified existing rules regarding communicating with other vendors or CNAs and the difference between CVE entries that are marked as disputed versus rejected.

- Defined additional terms, such as what it means for a vulnerability to be “public” and the definition of “hardware” within CVE and what hardware can receive CVE IDs.
- Set the CVE JSON format to be the preferred format for submitting CVE requests.
- Removed the CVE assignment requirement for Root CNAs, making it optional.
- A new rule indicating that CNAs must publish their CNA scope on their website as well as some other disclosure process information.

Become a CNA

CVE Blog | August 2, 2017

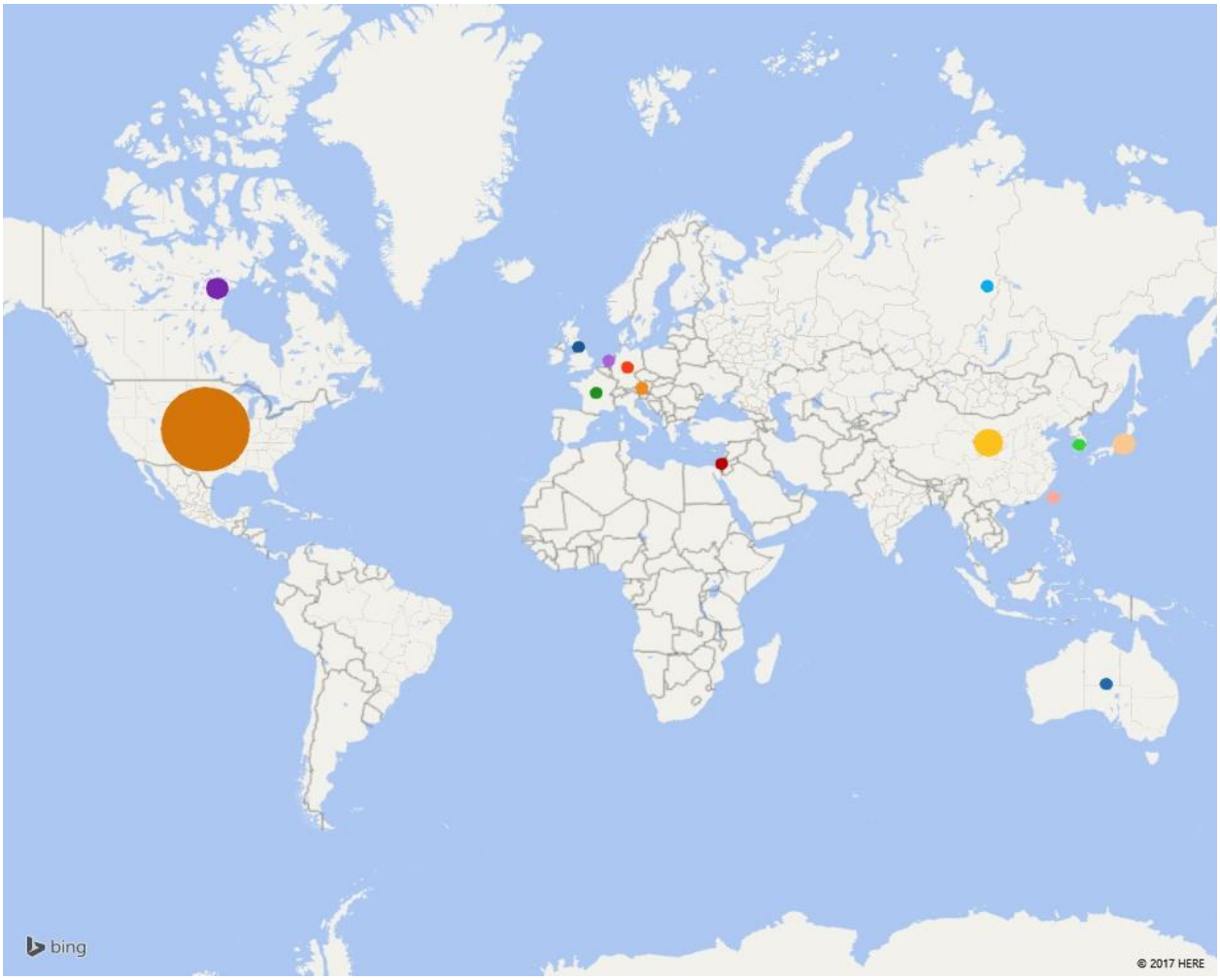
CVE Numbering Authorities, or “CNAs,” are how the CVE List is built. Every CVE Entry added to the list is assigned by a CNA.

The majority of CNAs are currently software vendors that assign CVE Entries to issues in their own products, but many vulnerability researchers and third-party coordinators also participate by assigning CVE IDs to issues in third-party products per their specified scopes of coverage. In all cases, by issuing CVE IDs themselves without directly involving MITRE in the details of the specific vulnerabilities, CNAs are able to ensure CVE IDs are available for inclusion in the first-time public announcement of a new vulnerability, which greatly benefits the overall cyber security community as organizations share information about the vulnerabilities and remediate them.

Actively Expanding the Number of CNAs

As of today, August 2, 2017, there are 69 total CNAs participating in the CVE program: 57 software vendors, 7 third-party coordinators, 4 vulnerability researchers, and MITRE as the Primary CNA.

And the CVE program has been actively growing the list of participating CNAs, which now includes organizations from around the world with 14 countries represented as illustrated in this map:



NUMBER OF CNAS BY COUNTRY, AS OF AUGUST 2017: Australia: 1; Austria: 1; Canada: 3; China: 6; France: 1; Germany: 1; Israel: 1; Japan: 3; Netherlands: 1; Russia: 1; South Korea: 1; Taiwan: 1; UK: 1; and USA: 47.

You too can become a CNA

Please consider joining us as a CNA. Participation 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.

If your organization would like to become a CNA, please follow these three steps:

1. Review the “CVE Numbering Authorities (CNA) Rules” document in its entirety.
2. Closely review the How to Become a CNA section of this website, which is excerpted from the “CNA Rules” above.
3. Contact us via our CVE Request web form by selecting “Other” from the dropdown menu.

We look forward to hearing from you!

Come Meet with CVE at *Black Hat 2017* on July 27 and *DEF CON 25* on July 28

CVE Blog | July 20, 2017

CVE Numbering Authority Program Lead Dan Adinolfi, and CVE Team Member Anthony Singleton, will be at *Black Hat USA 2017* and *DEF CON 25* next week in Las Vegas, Nevada, USA.

We invite you to join us to talk CVE at either or both events:

CVE Meet-Up, July 27

Please join us for an informal get together to talk CVE at *Black Hat USA 2017*. If you're interested, please meet us at 12:00 p.m. PT outside the House of Blues in the Mandalay Bay Casino.

We will determine the final location once we have everyone together. Questions or concerns: CVE Request Web Form - select “Other” from the dropdown.

CVE Talk, July 28

Dan and Anthony will present a talk entitled "CVE IDs and How to Get Them" at 1:10 p.m. PT in the Neopolitan Ballroom and Milano VIII at Caesars Palace at the "Wall of Sheep" at *DEF CON 25*.

Talk synopsis from the conference website:

> "The Common Vulnerabilities and Exposures (CVE) program uniquely identifies and names publicly-disclosed vulnerabilities in software and other codebases. Whether you are a vulnerability researcher, a vendor, or a project maintainer, it has never been easier to have CVE IDs assigned to vulnerabilities you are disclosing or coordinating around. This presentation will be an opportunity to find out how to participate as well as a chance to offer your thoughts, questions, or feedback about CVE. Attendees will learn what is considered a vulnerability for CVE, how to assign CVE IDs to vulnerabilities, how to describe those vulnerabilities within CVE ID entries, how to submit those assignments, and where to get more information about CVE assignment."

Please stop by either or both events and say hello. We look forward to seeing you!

Marking a CVE ID “REJECT” Is Not Permanent; It Can Be Updated and Added to the CVE List

CVE Blog | June 27, 2017

The CVE Team and CVE Board have recently revisited the use of CVE Identifier (CVE ID) states — REJECT, RESERVED, DISPUTED — and are planning to make some necessary changes to them in the coming months.

One of the changes recently discussed was in how the “REJECT” state is applied, and specifically whether a REJECT CVE ID can change states again at a later date.

What REJECT Means for a CVE ID

As a recap, a CVE ID marked as REJECT is a CVE ID that is not accepted as a CVE ID. The reason a CVE ID is marked REJECT will most often be stated in the Description of the CVE ID. Possible examples include it being a duplicate CVE ID, it being withdrawn by the original requester, it being assigned incorrectly, or some other administrative reason.

As a rule, REJECT CVE IDs should be ignored. However, there may be cases where a CVE ID previously marked as REJECT might need to move back to RESERVED or a populated state (i.e., the details and References are published and included).

A REJECT State Is Not Permanent

The CVE Team and CVE Board agree that the REJECT state should NOT be considered permanent, and that changes to this CVE ID state should be allowed in the future.
An example case could include a simple accidental REJECT, where a CVE ID was marked as REJECT by a CVE Numbering Authority (CNA) but the CVE ID was used publicly. In this case, it would create more confusion and additional work to REJECT the already used CVE ID, assign a new CVE ID, and also make sure that all public references are updated. The change discussed here would be to simply change the REJECT CVE ID and populate it with the details that were intended.

Both the CVE Team and CVE Board agree that some downstream consumers of CVE may be currently interpreting the REJECT state as permanent and that the CVE ID will never change in the future. It was also agreed that we should provide proper notice to the community that this change in use of the REJECT state should be provided.

Moving Forward

This announcement serves as notice that beginning **July 27, 2017**, CVE IDs in the REJECT state can be changed to another state at any time as appropriate.

Why Is a CVE Entry Marked as "RESERVED" When a CVE ID Is Being Publicly Used?

CVE Blog | May 10, 2017

A CVE Identifier (CVE ID) is marked as "RESERVED" when it has been reserved for use by a CVE Numbering Authority (CNA) or security researcher, but the details of it are not yet included in the CVE entry. Often, this is because the original requester of the CVE ID assignment has not sent an update to MITRE with the information needed to populate the CVE entry.

If you are aware of a CVE ID that is being used publicly but is not yet included in the CVE List, you can request that the CVE ID be updated through the CVE Request web form. MITRE will coordinate with the original requester to have the missing public information added to the entry.

CVE IDs are made public on countless forums, mailing lists, and other publications. CVE ID entries cannot be published without public references and other descriptive information. Searching the Internet for any public reference to a reserved CVE ID is a non-trivial problem to solve, and MITRE must rely on the community to assist with updating CVE information as it becomes public. MITRE is looking for new ways to automate and expand discovery processes, but the scale and breadth of the searchable space is growing exponentially. We hope that stakeholders will assist with this process by notifying MITRE when they see a discrepancy, and MITRE will work to quickly and accurately update outdated entries that are reported to them.

The Significance and Meaning of a CVE Identifier Marked as "RESERVED"

CVE Blog | March 16, 2017

A CVE Identifier (CVE ID) is marked as "RESERVED" when it has been reserved for use by a vendor or security researcher but the details of it are not yet populated by the requester.

A CVE ID can change from the RESERVED state to being populated at any time based on a number of factors both internal and external to MITRE.

An example of an internal factor could include the bulk assignment of CVE IDs to a CVE Numbering Authority (CNA). These CVE IDs are marked as RESERVED upon allocation to a CNA, before they are assigned to a specific vulnerability. An example of an external factor could include a vulnerability that have not yet been publicly disclosed, such as when the affected product vendor is still developing a mitigation.

It is also important to note that when a CVE ID is marked as RESERVED, it will not yet be available in the U.S. National Vulnerability Database (NVD). NVD is based-upon and fed by the CVE List.

However, once the CVE ID is populated with details and published on the CVE List on the CVE website, it will become available in NVD. As one of the final steps in the overall process, the NVD Common Vulnerability Scoring System (CVSS) scores for the CVE ID are assigned by the NIST NVD team.

Summary of Your Feedback About Updating Info in CVE ID Descriptions

CVE Blog | February 2, 2017

Thank you for your responses to our most recent post "What's your opinion on updating CVE ID Descriptions?" about whether or not CVE ID Descriptions should be updated as new information becomes available, or if we should we reject and recreate the CVE IDs instead.

Updating of CVE ID Descriptions Is Preferred

The majority of respondents indicated that updating CVE ID Descriptions with new information is preferable to rejecting and issuing new CVE IDs.

The goals of CVE entries are to help people find the information they need about a vulnerability and provide enough information to allow people to be confident they are talking about the same vulnerability. Ensuring that CVE entries contain the most recent information on a vulnerability, either by updating an existing CVE entry or rejecting and issuing a new CVE entry, supports these goals.

Moving Forward

As the CVE program continues to develop its policies and practices, we will consider the feedback from the CVE community on the benefits of updating CVE entries versus issuing new CVE entries.

Thank you again to all who participated.

The Significance and Meaning of the Year Portion of a CVE Identifier

CVE Blog | January 17, 2017

CVE Identifiers (CVE IDs) have the format CVE-YYYY-NNNNN. The YYYY portion is the year that the CVE ID was assigned OR the year the vulnerability was made public (if before the CVE ID was assigned).

The year portion is not used to indicate when the vulnerability was discovered, but only when it was made public or assigned.

Examples:

- A vulnerability is discovered in 2016, and a CVE ID is requested for that vulnerability in 2016. The CVE ID would be of the form "CVE-2016-NNNN".

- A vulnerability is discovered in 2015 and made public in 2016. If the CVE ID is requested in 2016, the CVE ID would be of the form "CVE-2016-NNNNN".

- A vulnerability is discovered in 2015 and a request is made for a CVE ID in 2015. The vulnerability is assigned "CVE-2015-NNNN" but not made public. (The CVE ID would appear as "Reserved" in the CVE ID list.) The discloser does not publish the CVE ID publicly until 2017, though. In this case, the CVE ID is still "CVE-2015-NNNN", despite the fact that the vulnerability isn't made public until 2017.

- A vulnerability is discovered and published in 2015 without having a CVE ID assigned to it. Someone requests that a CVE ID be assigned to the vulnerability in 2016. The vulnerability is given "CVE-2015-XXXX" since it was first made public in 2015.

NOTE: Neither the date when a vulnerability was introduced into a product, or the date when a vulnerability was fixed in a product, factor into what year is indicated in the CVE ID assigned to that vulnerability.