CVE Blog

Read more posts on CVE Website or Medium.

All CVE Blog articles published in calendar year 2019 are included in this single PDF.

Table of Contents:

- CVE Program Report for Calendar Year Q3-2019, November 18, 2019
- Become a CNA to Assign Your Own CVE IDs, August 29, 2019
- CVE Working Groups Overview, May 30, 2019
- Refresher: When to Use the CVE Request Web Form, January 2, 2019

CVE Program Report for Calendar Year Q3-2019

CVE Blog | November 18, 2019

The CVE Program will issue a summary of program milestones and metrics for each quarter of the calendar year (CY), beginning with the summary for CY Q3-2019, below.

CY Q3 Milestones

5 CVE Numbering Authorities (CNAs) Added
Five new CNAs were added: Bitdefender (Romania), GitHub (USA), HCL Software (India), OPPO (China), and Salesforce (USA). DUO merged with Cisco, which remains a CNA.

100+ CNAs Milestone Achieved
On August 14, the CVE Program achieved the milestone of 100 organizations participating as CNAs. By the end of CY Q3, there were 103 CNAs.

Added a New CVE Board Member from Trend Micro/ZDI
Shannon Sabens of Trend Micro Incorporated/Zero Day Initiative (ZDI) was elected to the CVE Board on July 2.

Added a New CVE Working Group Focused on Outreach and Communications
The Outreach and Communications Working Group (OCWG), formed in July, is focused on promoting the CVE Program to achieve program adoption and coverage goals through increased community awareness.

CVE Working Groups (WGs) Information Added to Main CVE Website
Information about contact methods, documents, and projects for the five CVE WGs—which are open to community participation—were added for the community on the CVE website. CVE WGs are actively focused on: automation, strategic planning, CNA coordination, CVE quality, and outreach and communications.

Began CVE 20-Year Anniversary Activities
The CVE Program began its 20-year anniversary by continuing ongoing engagement with the CVE and cybersecurity communities at *Black Hat USA 2019* on August 3-8, and *DEF CON 27* on August 8-11, in Las Vegas, Nevada, USA.

CY Q3 Metrics

Metrics for CY Q3-2019 populated CVE Entries, reserved CVE Entries, and requests for CVE IDs from the CVE Program Root CNA (currently MITRE), are included below. Annual metrics are also included in the charts for year-to-year comparisons.

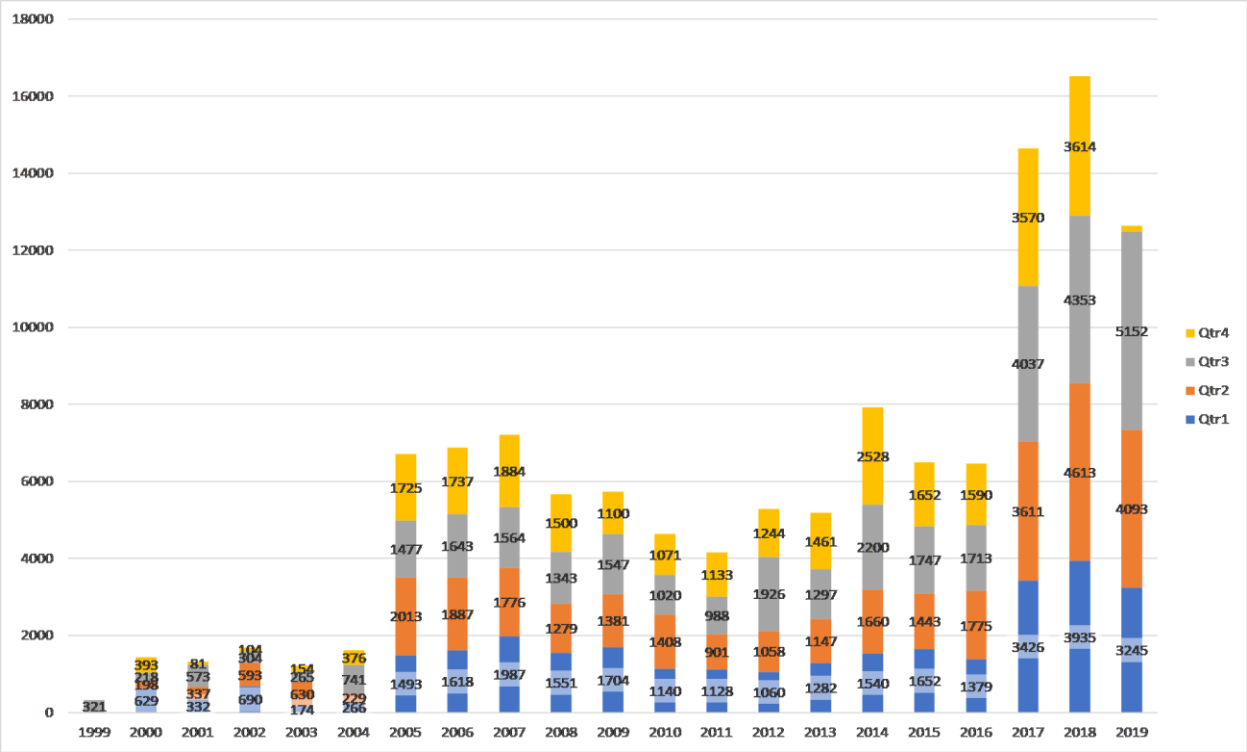
Terminology

- Populated – A populated CVE Entry includes the CVE ID, a brief description, and at least one public reference.
- Reserved – CNAs reserve a CVE ID for a given vulnerability prior to assigning and populating it as a CVE Entry on the CVE List.

Populated CVE Entries

As shown in the table below, CVE Program production was 30% above average in Q3 for this calendar year. This includes all CVE Entries populated by all CNAs. An average of 3,960 CVE Entries have been populated per quarter, year-to-date.

All CNAs Year-to-Date	
2019	Populated CVE Entries
Q1	3,245
Q2	4,093
Q3	5,152

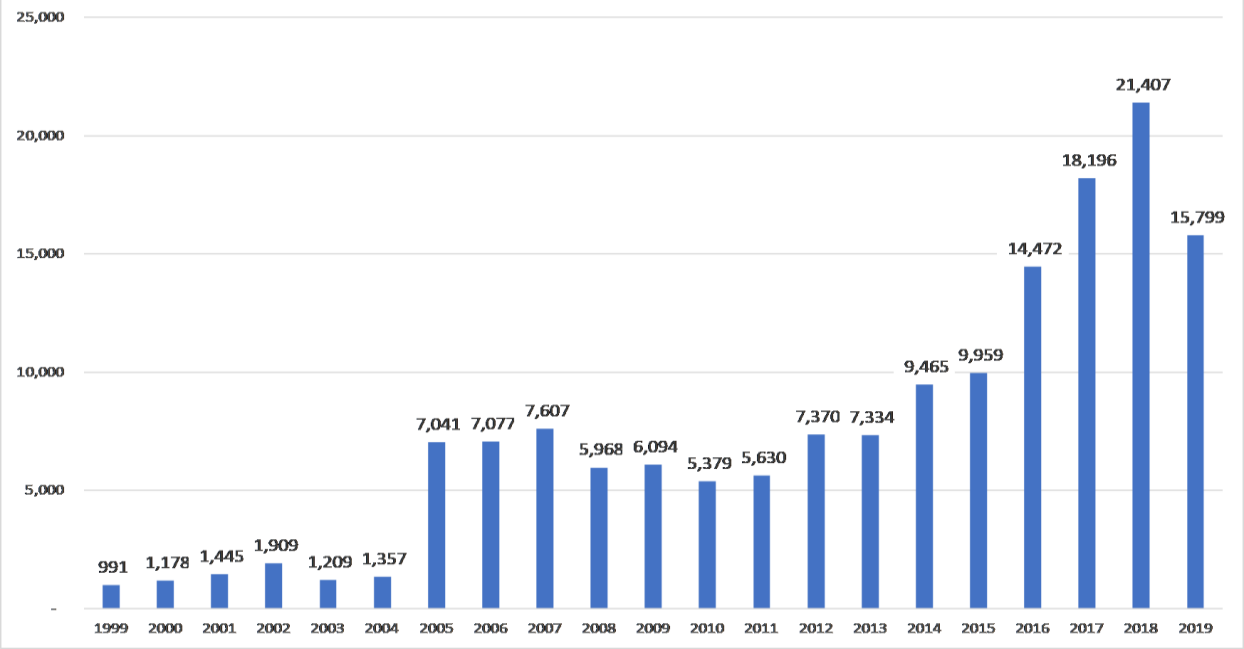


Comparison of Populated CVE Entries by Year for All Quarters (figure 1)

Reserved CVE Entries

The CVE Program tracks reserved CVE Entries. As shown in the table below, the number of CVE IDs in the reserved state for Q3 is 10.7% above the previous quarter. The chart below (figure 2) shows the number of CVE IDs added to the CVE List for each year. As we are still in 2019, only the number of CVE IDs before October are shown for 2019. Unlike the table, the CVE IDs in the chart can be either in the reserved or populated state.

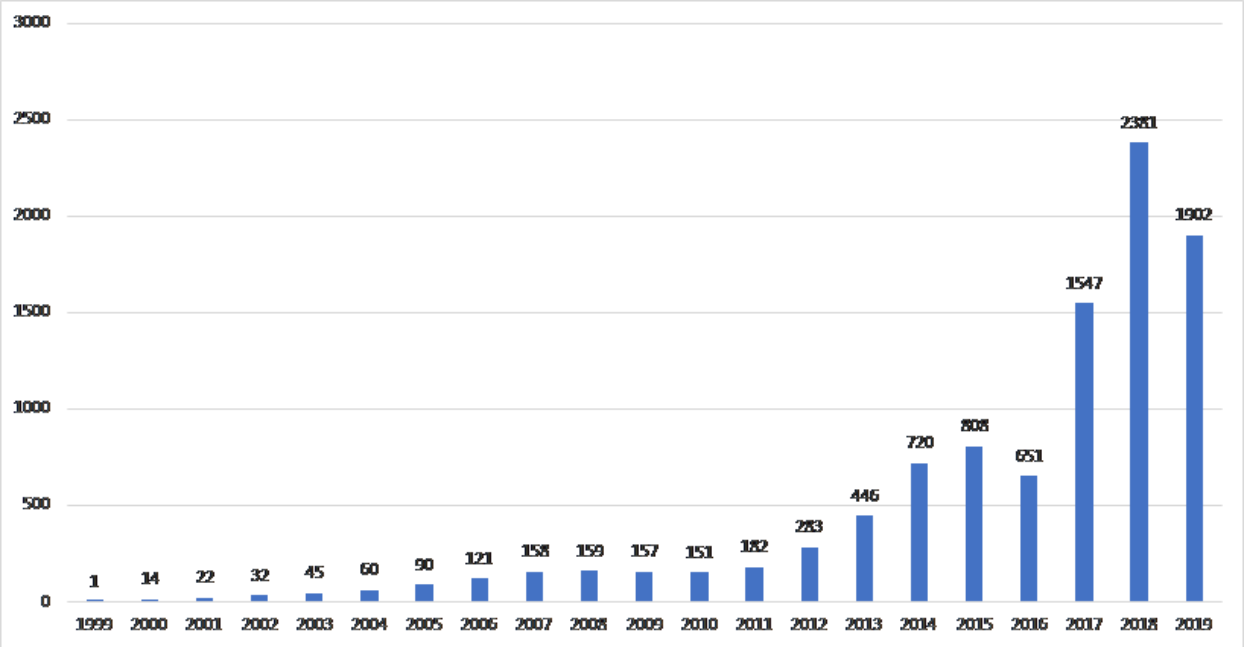
All CNAs Year-to-Date	
2019	Reserved CVE IDs
Q1	7,818
Q2	2,572
Q3	5,345



Comparison of Reserved CVE Entries by Year for All Quarters - All CNAs Year-to-Date CYQ32019 (figure 2)

Requests for CVE IDs from the Program Root CNA

Finally, the CVE Program Root CNA receives requests for CVE IDs from the community for vulnerabilities and open source software product vulnerabilities that are not already covered by another CNA. The chart below shows the number of unique requesters that received one or more CVE IDs from the Program Root CNA as of CY Q3-2019, as well as by year.



Requesters that Received a CVE ID from Program Root CNA for CYQ32019 and All Years (figure 3)

All CVE Entries Are Assigned by CNAs

All of the CVE Entries cited in the metrics above are assigned by CNAs. CNAs are software vendors, open source projects, coordination centers, bug bounty service providers, and

research groups authorized by the CVE Program to assign CVE Entries to vulnerabilities within their own specific scopes of coverage. CNAs join the program from a variety of business sectors; there are minimal requirements, and there is no monetary fee or contract to sign.

Currently, 107 organizations from 20 countries are actively participating in the CVE Program as CNAs. Learn how to become a CNA.

Comments or Questions?

If you have any questions about this article, please use the CVE Request Web Form and select "Other" from the dropdown menu. We look forward to hearing from you!

Become a CNA to Assign Your Own CVE IDs

CVE Blog | August 29, 2019

CVE Numbering Authorities, or "CNAs," are organizations authorized to assign and populate CVE Entries to vulnerabilities affecting products within their distinct, agreed-upon scope.

A CNA may be a software vendor, open source project, coordination center, bug bounty service provider, or research group. CNAs are essential to the CVE Program's success and every CVE Entry added to the CVE List is added by a CNA.

Benefits of Being a CNA

Currently, 101 organizations from around the world are actively participating in the CVE Program as CNAs. There is no monetary fee and no contract to sign to become a CNA. CNAs volunteer their own time for their own benefit.

The only requirements are to have a public vulnerability disclosure policy and a public source for new vulnerability disclosures, to agree to the CVE Terms of Use, and agree to follow the program's rules and guidelines.

Becoming a CNA allows you to:

- Demonstrate mature vulnerability management practices and a commitment to cybersecurity to current and potential customers.
- Communicate value-added vulnerability information to your customer base.
- Control the CVE publication release process for vulnerabilities in your scope.
- Assign CVE IDs without having to share embargoed information with another CNA.
- Streamline your vulnerability disclosure processes.
- CNAs are also able to participate in other aspects of the CVE Program. Examples include influencing the CNA rules and guidelines upon which the program operates, and joining one or more of the CVE Working Groups to help improve CVE workflows and processes.

How to Become a CNA

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

1. Contact the CNA Coordination Team.
2. Fill out the registration form.
3. Attend an introductory session.
4. Successfully create CVE ID entries from examples.

Comments or Questions?

If you have any questions, or would like to start the process, please use our CVE Request Web Form and select “Request information on the CVE Numbering Authority (CNA) Program” from the dropdown. We look forward to hearing from you!

CVE Working Groups Overview

CVE Blog | May 30, 2019

The CVE Program has a number of Working Groups (WGs) actively focused on improving processes, workflows, and other aspects of the program as CVE continues to grow and expand. You may request to join a WG, or request more information, by using the CVE Request Web Form and selecting “Other” from the dropdown.

Current documents, repositories, and projects for CVE’s WGs are included below. Updates to this information will be posted on the CVE Working Groups page.

Automation Working Group (AWG)

Focused on identifying and advancing proposals for the collaborative design, development, and deployment of automated capabilities that support the efficient management of the CVE Program.

Documents:

- CVE ID Allocation Service Specification
- AWG Charter

Repository:

- AWG GitHub Repository

Projects:

- CVE ID Allocation Service
- CVE List GitHub Automation Pilot
- CVE JSON Schema Project
- CNA Registry Project

Strategic Planning Working Group (SPWG)

Focused on the long-term strategy (1-5 years) and goals of the CVE Program; will work closely with the CVE Board to determine goals and objectives and will act to achieve them.

Repository:

- SPWG GitHub Repository

CNA Coordination Working Group (CNACWG)

Focused on providing a forum for more effective communication and participation by the CVE Numbering Authorities (CNAs).

Documents:

- CNACWG Charter

CVE Quality Working Group (QWG)

Focused on identifying areas where CVE content, rules, guidelines, and best practices must improve to better support stakeholder use cases.

CVE Outreach and Communications Working Group (OCWG)

Focused on promoting the CVE Program to achieve program adoption and coverage goals through increased community awareness.

To discuss this post with us, please use our LinkedIn page or the CVE Request Web Form by selecting “Other” from the dropdown. We look forward to hearing from you!

Refresher: When to Use the CVE Request Web Form

CVE Blog | January 2, 2019

First introduced in August 2016, the online “CVE Request Web Form” is the main method for communicating with the CVE Program Root CNA. By using the web form, the CVE Program’s ability to receive, manage, track, and respond to user questions and CVE ID requests has significantly improved.

In this article, inspired by user questions, we will discuss when and how to use the CVE Request Web Form to best assist you.

Only Use the CVE Request Web Form to Contact the Program Root CNA

Each CVE Numbering Authority (CNA) has its own specific scope of coverage, and its own preferred way to be contacted. If you need to contact a CNA other than the Program Root CNA to request a CVE ID, or to ask a question, please use that specific CNA's contact details as stated on the Request CVE IDs page.

The CVE Request Web Form is only used to contact the Program Root CNA.

When to Use the CVE Request Web Form

Use the web form to contact the Program Root CNA to do the following:

- **Request a CVE ID**

  Select this option to request a CVE ID(s) from the Program Root CNA only. The form includes a required information section for the type of vulnerability, product vendor name, and affected product name and version. There is also an optional information section to fill out that may assist us in processing your request.

  If you are unsure about a web form requirement, or need further clarification before starting the process, please continue to use the web form but select "Other" from the dropdown menu to ask us your question(s).

- **Request a block of IDs (for CNAs only)**

  Only current CNAs may use this selection to request blocks of CVE IDs.

- **Notify CVE about a publication**

  Select this option to notify the CVE Team that an advisory has been published. Required information includes providing a URL to the public advisory about the vulnerability, listing the CVE ID(s) that are included in the advisory, and any additional information and CVE ID Description updates.

- **Request an update to an existing CVE Entry**

  Select this option to provide updates for published CVE Entries. Required information includes the type of update (duplicate, rejection, split/merge, update description, update references, or other), the CVE ID of the CVE Entry to be updated, and a description of what change is needed. Optional information includes providing links to references that validate the need for an update.

- **Request information on the CVE Numbering Authority (CNA) Program**

  After reviewing the CVE Overview for Prospective CNAs and How to Become a CNA, select this option to find out more or to start the process of becoming a CNA.

- **Other**

Select to ask questions about CVE IDs, CVE Entries, the ID request process, the web form, or to request information on topics not covered above.

If you need additional information regarding how use the web form, the form itself includes online help during each step of the process. Simply click the round, blue information button containing the letter "i". Please also see our Web Form FAQs.

What Happens Once a Request Is Submitted

Once you have submitted your request, you will receive an email message confirming receipt of your request and a reference number. Please add cve-request@mitre.org and cve@mitre.org as safe senders in your email client before completing the web form.

Any additional communications related to this request will be done through email using the same subject line as the confirmation email.

Did We Point You in the Right Direction?

To discuss this post with us, please use our LinkedIn page or the CVE Request Web Form by selecting “Other” from the dropdown. We look forward to hearing from you!