Common Vulnerabilities and Exposures (CVE) Program Overview

Introduction

This document provides an overview of the Common Vulnerabilities and Exposures (CVE) Program, including a description of the CVE Identifier (ID) numbering process, the CVE Numbering Authority (CNA) Program, the CVE Program’s administrative structure, and the requirements to participate as a CNA. CVE is sponsored by the Department of Homeland Security (DHS) Office of Cybersecurity & Communications (CS&C) United States Computer Emergency Readiness Team (US-CERT). MITRE operates the Homeland Security Systems Engineering and Development Institute (HSSEDI) Federally Funded Research and Development Center (FFRDC) and participates in the CVE Program in this capacity. Specifically, MITRE is a member of the CVE Board, and serves as the CVE Board moderator and the Primary CNA. In addition, MITRE copyrighted the CVE List for the benefit of the community in order to ensure it remains a free and open standard, as well as to legally protect the ongoing use of it, and any resulting content, by government, vendors, and users.

CVE Program Overview

The CVE Program provides the public with a means to document and uniquely identify a subset of the publicly disclosed vulnerabilities pertaining to specific versions of software or codebases. Unique CVE IDs allow for a common reference, with the CVE List serving as a dictionary of publicly known cybersecurity vulnerabilities[[1]](#footnote-1). The CVE Program provides a pivot point between vulnerability scanners, vendor patch information, patch managers, and network/cyber operations. Referencing a CVE ID, stakeholders can have confidence that they are talking about a specific, unique vulnerability, regardless of the tool or forum being used. CVE is free to use and publicly available to anyone interested in correlating data between different vulnerability or security tools, repositories, and services.

The current scope of the CVE Program is the Information Technology (IT) Sector.[[2]](#footnote-2) The Program’s goal is to expand both within the IT Sector, and to other domains. To achieve this goal, the program will use the knowledge and experience both resident within the program itself, and the vulnerability management community writ-large. For program expansion to occur, additional considerations are necessary. For example, a given domain may have its own vulnerability description syntax, content requirements, domain administration of vulnerability management, and funding source(s). In addition, different regulatory, legal, and practical considerations within a domain may affect the governance model within that domain.

Ultimately, the CVE Program seeks to work closely with global vulnerability management communities in all domains. As the CVE Program evolves and grows, it must address the needs of the global community for: unique vulnerability identification covering critical infrastructure and key resources within the IT sector and beyond; a community of experts with committed participation in vulnerability management for each domain; a process for those experts to follow that ensures repeatability and support within and across domains; and finally, a means to evolve the processes to accommodate changes.

CVE ID Assignment Process

Figure 1, below, highlights the current high-level process for assignment of CVE IDs. Researchers or vendors who discover a vulnerability request a CVE ID from a CVE Numbering Authority (CNA). The vulnerability is made public by the researcher or vendor and the CVE entry is developed.

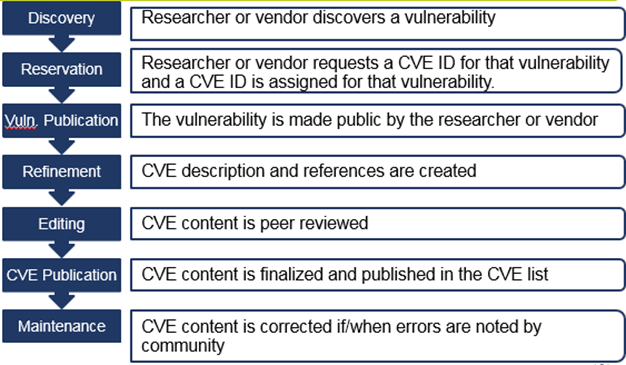


Figure 1. High Level CVE ID Assignment Process

Figure 2 below provides an example of a CVE entry. CVE entries contain the CVE ID, a description of the vulnerability and references to public disclosure sources. After the CVE entry is completed, it is peer reviewed by the CNA analyst before being finalized and published in the CVE List. If errors are found, or new references identified, the CVE entry may be updated or rejected by MITRE.

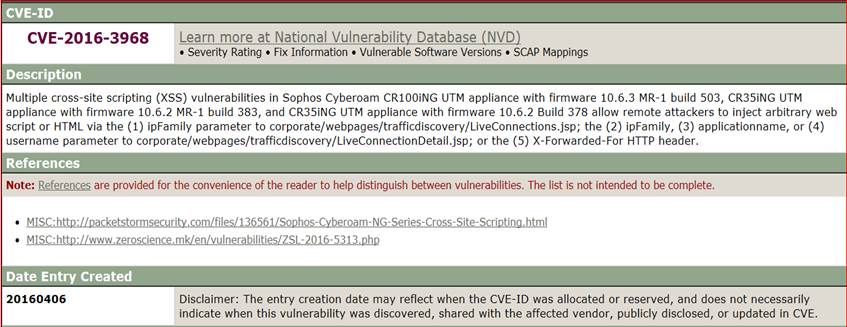


Figure 2. CVE Example

It is important to note that the CVE is not a tool for the initial public disclosure of vulnerabilities; that is, only vulnerabilities that have already been publicly disclosed and are within the CVE scope are included in the CVE list. In addition, it is not a source for vulnerability risk, impact, fix, or technical information. CVE entries do not provide a vulnerability mitigation.[[3]](#footnote-3) CVE IDs can be used to access fix information in separate CVE-compatible databases. For example, the National Vulnerability Database (NVD), will reference CVE information and provide more enhanced information, such as fix information, severity scores, and impact ratings.

CVE Numbering Authority (CNA) Program

CNAs are organizations that assign and publish CVE ID numbers for vulnerabilities that will be made public. CNAs assign CVE IDs, in accordance with CNA Rules, to researchers and vendors for inclusion in their first-time public announcements of new vulnerabilities. Each CNA has a specific scope[[4]](#footnote-4) of responsibility, delimiting what products, information sources, or domains for which they assign CVEs IDs.

The CNA Program provides CNAs with a set of documentation that includes CNA Rules and Responsibilities, operational guidelines, and policy and process templates. The CNA Program provides specific scope to individual CNAs and designation as a Root or Sub-CNA (described below) as of 2017.

There are several benefits to becoming a CNA. First, CNAs do not have to wait for a CVE ID assignment from another entity. This allows them the ability to publicly disclose new vulnerabilities with CVE IDs assigned to them at the time of disclosure. In addition, CNAs can better control their vulnerability management process through the use of CVE Program provided tools. CNAs benefit from direct notification of vulnerabilities in the organization’s products by researchers who must request a CVE ID from them. Finally, the CVE Program provides various forums, such as the CVE Board, the CNA Working Group, the CNA community mailing list and periodic CNA community meetings, through which CNAs can collaborate with other CNAs within their domain and across the CNA program Administrative Structure.

CVE Program Administrative Structure

The vision of the CVE Program is to evolve into a global, federated system of vulnerability identifiers, with a defined common naming convention and an active and engaged set of collaborating community and domain publishers, each of whom operate according to their specific use cases for vulnerability identification and definition.

**The Vision**

**A global, federated system of vulnerability identifiers evolved from today’s CVE, with a defined common naming convention and an *active and engaged* set of collaborating community and domain publishers, each of whom operate according to their specific use cases for vulnerability identification and definition.**

The federated structure, shown in Figure 2 below, consists of multiple Sub-CNAs operating under the oversight of a Root CNA, while the Root CNAs operate under the oversight of a single, Primary CNA. Sub-CNAs coordinate with their Root CNA or the Primary CNA to ensure the CNA analysts are properly trained, and all roles and responsibilities will be satisfied at an appropriate level of quality. Currently, the MITRE Corporation is the only Primary CNA.

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 within that domain or community. Sub-CNAs only assign CVEs for vulnerabilities in their own products or their domain of responsibility.

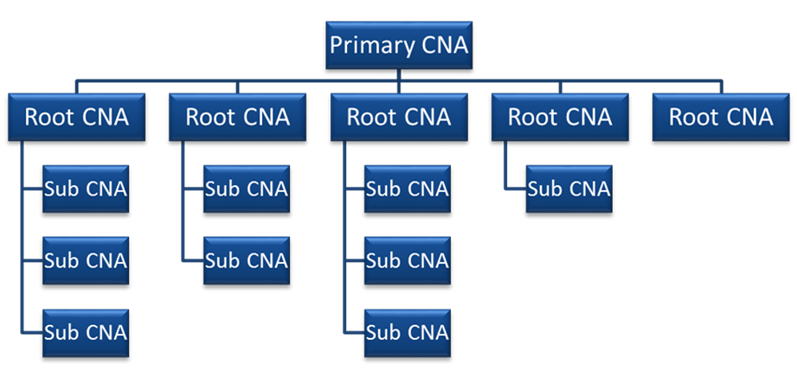


Figure 3. Administrative Structure

As the Primary CNA, the MITRE Corporation operates the CVE Program, manages Root CNAs, trains and admits new Root CNAs, and is the assigner of last resort for requesters that are unable to have CVE IDs assigned at the Root or Sub-CNA levels.

By increasing the CNA network through the federated structure, the CVE program seeks to satisfy the CVE community’s need for an increase in the number of CVE IDs to match the increase in the number of vulnerabilities and for timely CVE ID assignment of those CVE IDs. The federated structure also supports expansion of the CVE Program’s scope to other domains and to address the evolving state of global vulnerability management.

Participating as a CNA

Currently, the CVE Program requires that CNAs must be a major software vendor with a significant user base and an established security advisory capability, or an established third party that typically acts as a neutral interface between researchers and vendors. The CNA must be an established distribution point for first-time vulnerability announcements.

There is no cost to participate in the CNA program beyond the internal operational costs of assigning CVE IDs and communicating with the CNA community and external disclosers.

For more information on how to participate as a CNA contact CVE at [cve@mitre.org](mailto:cve@mitre.org) or visit <http://cve.mitre.org>/.

1. A vulnerability in the context of the CVE Program, is defined as a weakness in the computational logic (e.g., code) found in software and some hardware components that, when exploited, results in a negative impact to confidentiality, integrity, or availability. [↑](#footnote-ref-1)
2. <https://www.dhs.gov/critical-infrastructure-sectors> [↑](#footnote-ref-2)
3. Mitigation of the vulnerabilities in this context typically involve coding changes, but could also include specification changes, or even specification deprecations (e.g., removal of affected protocols or functionality in their entirety). [↑](#footnote-ref-3)
4. [https://cve.mitre.org/cve/cna.html#participating\_cnas](%20https:/cve.mitre.org/cve/cna.html%23participating_cnas) [↑](#footnote-ref-4)