CVE Overview for Prospective CNAs

September 29, 2017

Version 1.0

Contents

List of Figures

1 Introduction

The Common Vulnerabilities and Exposures (CVE®)[1] List is a dictionary of publicly disclosed vulnerabilities that is free for use and download. The CVE List is a collection of CVE Entries that provide a unique identifier for each vulnerability, the "CVE ID"; a standardized description; and a set of references. The CVE List is restricted to publicly-available vulnerability information to ensure that it addresses the needs of the largest possible segment of the cybersecurity community rather than closed, focused sub-groups. The unique CVE ID provides a point of reference among other names, enabling the cross-matching or deconfliction among names, thereby avoiding conflicts and confusion.

The demand for CVE IDs and associated information is such that successful operation of the CVE Program requires more than one CVE assigning authority. To satisfy that demand and to ensure its continued success, the CVE Program utilizes multiple cooperating CVE Numbering Authorities, or CNAs. CNAs today include major operating system (OS) and application vendors and maintainers, hardware development vendors, computer emergency response teams (CERTs), security researchers, and research organizations. These assignments are made by the CNAs without directly involving the Primary CNA in the details of the specific vulnerabilities, enabling the inclusion of an assigned CVE ID with the first public disclosure of a vulnerability. To be successful, CNAs must be aware of the potential complexities of creating CVE Entries and must abide by defined rules and practices to ensure consistency across the CVE List.

This document describes the design and operation of the CVE Program and List, and some of the considerations that a CNA might encounter. The intent of this document is to describe the roles and responsibilities of a CNA such that a decision can be made whether to pursue becoming a CNA.

2 Conceptual Basis of CVE

Leading up to the creation of CVE, MITRE documented "Four Roadblocks to Interoperability" [1]:

1. Inconsistent Naming Conventions
2. Managing Similar Information from Diverse Sources
3. Managing Multiple Evolving Perspectives of the Same Vulnerability
4. Complexity of Mapping Between Databases

A critical insight enabling the CVE Program was that "naming precedes organization." By assigning essentially meaningless "names" for vulnerabilities and collecting them in a list, users can understand and exchange vulnerability information almost without regard to its provenance.

[1] CVE and the CVE logo are registered trademarks of The MITRE Corporation (2002, McLean, VA USA).

3 Design and Operational Choices for CVE

The limited amount of information in a CVE Entry can cause confusion for those new to the CVE Program and for prospective CNAs. There is often an expectation that a CVE Entry provides a much richer set of information about a vulnerability. These limitations are intentional and are in keeping with the design goals of the CVE Program. Most importantly, they are essential to the successful operation and broad utility of CVE.

The CVE Program was designed to do one thing and to do it well – provide a list (dictionary) of unique vulnerabilities. As originally proposed:

> "… a CVE should exist independently of the multiple perspectives of vulnerabilities. One way to ensure the independence of a CVE is to define vulnerabilities with only the necessary and sufficient attributes that are common to all vulnerabilities, ensuring that these attributes do not rely on any evolving representation and can be commonly agreed to by the majority of the security community" [1].

3.1 CVEs Purposely Provide Minimal Information About a Vulnerability

In the design of the CVE Program, it was proposed that the only essential elements of a useful CVE Entry are a unique CVE ID and a description with enough information to be able to differentiate between any two CVE Entries. This has proven to be critical to CVE's success. Being based on a unique ID and pertinent description enables CVE to "reduce the complexity… and avoid problems of representation and classification" [1]. As the development of the CVE Program progressed, it was determined that reference URLs for additional information regarding the subject vulnerability were necessary, allowing users to seek more details as needed.

3.2 The CVE List is a Simple List

It is critical to recognize that the CVE List is designed as a simple list or dictionary, rather than a database. As noted earlier, attempts to specify an exact representation or to classify a vulnerability result in disagreements about the choices made and the results, which prevents CVE from achieving its goal of maximum utility to the largest possible number of users.

3.3 CVE Only Publishes Already-Disclosed Vulnerabilities

By definition, the CVE Program only publishes information for a vulnerability that has already been publicly disclosed. However, for CNAs, there is a nuance that must be recognized – the CVE program may handle or otherwise be aware of a vulnerability before it is disclosed, but that information is never shared or discussed with anyone other than the discloser until the disclosure is made public. CNAs, for example, can and should assign CVE IDs to vulnerabilities only they know about, but those vulnerabilities and associated CVE IDs will only be published in the CVE List after those vulnerabilities have been made public. For CNAs, this means that the CNA must notify the MITRE CVE Team when a specific vulnerability has been publicly disclosed; the CVE Team does not generally look for previously unknown, disclosed vulnerabilities that have associated, unpublished CVE IDs.

3.4 The Anatomy of a CVE Entry - Example

A CVE Entry must contain three elements: (1) a unique CVE ID, (2) a short description, and (3) external references, as shown in the following example.

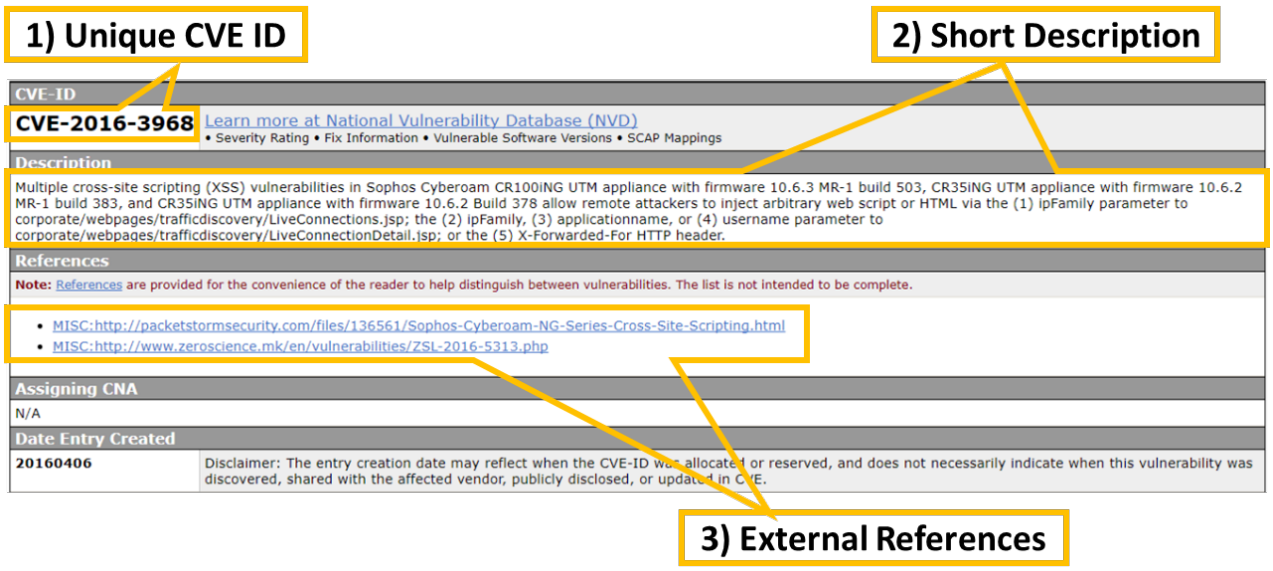

Figure 1: Sample CVE Entry

4 CVE and the National Vulnerability Database (NVD)

The purpose and function of the CVE Program and NVD are often confused, and they are not the same. The full CVE List is available from both CVE and NVD, and many users get CVE Entries directly from NVD without visiting the CVE website. The reference copy of the CVE List is maintained by MITRE on the CVE website, although NVD receives regular, timely updates of new or revised CVE Entries. As noted above, CVE does not itself provide or otherwise augment any information about a vulnerability other than the CVE ID, description, and references.

NVD, on the other hand, was designed to enable the "…automation of vulnerability management, security measurement, and compliance" [2]. As such, NVD uses CVE as one source of information it collects and publishes. NVD is a prime example of using the CVE List as a foundation for creating other capabilities and information sources to serve the cybersecurity community's needs.[2]

[2] See: https://cve.mitre.org/about/faqs.html#cve_nvd_relationship

5 CVE and CNAs

5.1 Sources of Vulnerability Information

The CVE Program has employed both automated collection of vulnerability information from specific web sites and direct submissions and requests from vendors, researchers, and other members of the cybersecurity community. The demand for both the number and timeliness of CVE IDs outstripped the ability of the CVE Program to keep up with the community's needs. In addition, it was clear that software vendors and sources are most qualified to assign their own CVE IDs, enabling greater coverage for the community.

An important note: although the CVE Program only publishes publicly available vulnerabilities, CVE IDs are often provided to disclosers by CNAs prior to announcements. These CVE IDs are marked as "RESERVED" to indicate that the CVE ID has been reserved for use by a CNA or security researcher, but the details of it are not yet populated. Note that a CVE Entry cannot be populated with details until a public reference exists that describes the vulnerability.

5.2 Benefits of Early CVE ID Assignment

There are two significant benefits to the community that are enabled by the early assignment of a CVE ID. First, if a CVE ID is available at the time of disclosure, it provides an immediate reference to an issue before publication in the CVE List. In addition, early, pre-publication assignment and use of CVE IDs enables response teams and other users to communicate and coordinate their efforts regarding a specific vulnerability prior to its formal publication.

5.3 Roles and Responsibilities of a CVE CNA – High Level View

CNAs are entities that are authorized to assign CVE IDs. MITRE currently functions as the Primary CNA and operates the CVE CNA program. A given CNA may only assign CVE IDs to vulnerabilities within that CNA's specific, documented scope. CNAs cannot assign CVE IDs outside of their scope, which prevents overlaps and confusion regarding CNA authority. CNAs must conform to the CNA rules for operation and assignment. Failure to do so may result in the revocation of a CNA's authority to assign CVE IDs.

Within their scope, CNAs can assign CVE IDs to multiple kinds of requesters, including (but not limited to) vendors of IT technology or IT technology-using products, vulnerability researchers, and other entities wishing to disclose a vulnerability. CNAs assign CVE IDs without directly involving the Primary CNA in the details of the specific vulnerabilities. Participation in the CNA program is completely voluntary, has no fee for inclusion in the program, and has no compensation from the CVE Program.

5.4 Benefits of Operating as a CNA

Operating as a CNA benefits the cybersecurity community, the CVE Program, and the organization operating the CNA itself. As noted, CNAs enable the timely disclosure of a vulnerability with an associated CVE ID. A CNA is also able to directly control pre-disclosure information for vulnerabilities in their assigned scope and is able to receive early notification of vulnerabilities in products within their scope – an important capability for those CNAs who are product vendors. Finally, being a CNA allows the assignment of a CVE ID without having to

request an ID from the MITRE CVE Team at the time of assignment, accelerating the disclosure process.

6 Special Considerations for Prospective CNAs

Becoming a CNA brings with it considerations and responsibilities that ensure the continuing quality of the CVE List and improving CVE's operation and timeliness.

6.1 Requirements for Assigning a CVE ID

The CVE List is not a database but is instead a list, or dictionary, of CVE Entries created according to specific, documented rules [3]. CVE ID assignments should be written in a way that prevents inconsistencies and thus degradation of the CVE List. While it may appear simple, this can be very challenging.

The correct assignment of a CVE ID requires that the ID and associated vulnerability:

1. Be assigned a standard, guaranteed-unique CVE ID;
2. Support discrimination among all publicly known vulnerabilities;
3. Exist independent of multiple possible perspectives of the subject vulnerability; and
4. Be assigned to a vulnerability that is or will be public, open, and shareable without any restrictions of any kind.

6.2 Challenges When Assigning CVE IDs

CNAs are required to make several judgements before assigning a CVE ID. For example, CNAs must determine whether the reported issue is even something that should be included in the CVE List; that is, identifying that the reported issue is truly a vulnerability or exposure and not something else, such as a system configuration issue. CNAs must also ensure that the vulnerability is included within that CNA's specific scope [3].

CNAs must be mindful of counting issues and adhere to the published rules [3]. This includes determining if the reported vulnerability is actually a single vulnerability or if it is a combination of several vulnerabilities, as well as the reverse case, where several reported vulnerabilities are in reality a single vulnerability.

CNAs must avoid duplicate reporting and must be especially mindful of the "rediscovery" of a previously reported problem.

CNAs must make every effort to abide by the published guidelines [3] to maintain consistency and accuracy within the CVE List, as well as their ability to operate as a CNA.

7 More Information

For more detailed information on the CNA program and on becoming a CNA, please see the CNA collection pages at: https://cve.mitre.org/cve/cna.html. [4]

8 List of Acronyms

Acronym	Definition
CNA	CVE Numbering Authority
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
FIRST	Forum of Incident Response and Security Teams
ID	Identifier
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database

9 References

[1] D. E. Mann and S. M. Christey, *Towards a Common Enumeration of Vulnerabilities,* Bedford, MA: The MITRE Corporation, 1999. [Online]. Available: https://www.cve.mitre.org/docs/docs-2000/cerias.html

[2] National institute of Standards and Technology, "National Vulnerability Database (NVD)," [Online]. Available: https://nvd.nist.gov.

[3] The MITRE Corporation, "CNA Rules v1.1," 16 September 2016. [Online]. Available: https://cve.mitre.org/cve/cna/CNA_Rules_v1.1.pdf.

[4] The MITRE Corporation, "CVE Numbering Authorities," [Online]. Available: https://cve.mitre.org/cve/cna.html#documentation_for_cnas.