CVE Program Glossary Revision 2024-01

Summary

In revising the CNA Operational Rules, it was decided to remove terms and definitions from the Rules document and integrate them with the existing CVE Glossary. This is a first but significant step towards having CVE Program-wide terms in one canonical place instead of scattered across multiple documents.

Proposed Glossary Updates

Council of Roots (CoR): The group of TL-Roots responsible for governance and administration of their respective hierarchies.

CVE: The CVE registered trademark and the name Common Vulnerabilities and Exposures.

CVE Board: The organization responsible for the strategic direction, governance, operational structure, policies, and rules of the CVE Program.

CVE Identifier (CVE ID): An alphanumeric string that identifies a Publicly Disclosed vulnerability. The format of the CVE ID is defined in the CVE Record Format.

CVE List: The catalog of all published CVE Records.

CVE Numbering Authority (CNA): An authorized entity with specific scope and responsibility to regularly assign CVE IDs and publish corresponding CVE Records.

CVE Numbering Authority of Last Resort (CNA-LR): A CNA authorized by a Root to assign CVE IDs and to publish corresponding CVE Records within that Root's scope for vulnerabilities not covered by the Scope of another CNA.

CVE Program: An international, community-driven effort to identify and catalog publicly disclosed vulnerabilities.

CVE Record: Structured data about a Vulnerability associated with a CVE ID. CVE Records are authored by CNAs. A CVE Record can be in one of the following states:

- Reserved: A CNA has reserved a CVE ID. This is the initial state of a CVE ID.
- Published: A CNA has populated the data associated with the CVE ID and published the CVE Record.

- Rejected: The CVE ID and the associated CVE Record should no longer be used. A Rejected CVE Record remains on the CVE List so that users know that the CVE ID and CVE Record are invalid.

CVE Working Group: An organization created and administered by the CVE Board to accomplish specific objectives through collaboration with CVE stakeholders and the general public where appropriate.

End of Life (EOL): A Product that no longer receives security Fixes. EOL typically indicates that a Product no longer receives any support, maintenance, or new features.

Fix: A change to software to remediate, mitigate, or otherwise address a vulnerability. “Fix” is used broadly and includes terms such as patch, fix, hotfix, update, and upgrade.

Independently Fixable: A vulnerability is independently fixable when it can be fixed without fixing a separate vulnerability.

Product: A unit of software or hardware or both. “Product” is used broadly and includes services, open source projects, specifications, and other common terms such as: system, appliance, device, component, library, package, archive, and collection.

Publicly Disclosed: The state in which non-trivial information about a vulnerability is publicly available. The publication of most vulnerability advisories, software updates, proof-of-concept exploit code, or other detailed information makes the vulnerability “Publicly Disclosed.”

Reserved but Public (RBP): A CVE ID in the “Reserved” state that is referenced in one or more public sources but for which a CVE Record has not been published.

Root: An organization authorized within the CVE Program that is responsible, within a specific Scope, for the recruitment, training, and governance of one or more entities that are a CNA, CNA-LR, or another Root.

Scope (Scope Definition): A defined set of products, vulnerabilities, or both for which a CNA has authority and responsibility.

Secretariat: An organization authorized by the CVE Program to develop, host, and maintain the Program’s infrastructure and to provide administrative and logistical support for the CVE Board, CVE Working Groups, and other parts of the Program.

Tags: Labels used to indicate defined characteristics of CVE IDs.

- exclusively-hosted-service: All known Products affected by the CVE ID exist only as fully hosted services. If the vulnerability affects both hosted services and on-premises Products, then this tag should not be used.
- unsupported-when-assigned: At the time of CVE ID assignment, all known Products affected by the CVE ID no longer receive security Fixes. Typically the Products are no longer supported and are considered to be End of Life (EOL).

- disputed: A CVE ID assignment or CVE Record content have been disputed.

Supplier: The entity that develops, maintains, or provides a product. A supplier is typically responsible for and capable of investigating vulnerability reports and developing fixes or mitigations for vulnerabilities. “Supplier” is used broadly and includes common terms such as vendor, producer, developer, maintainer, author, owner, manufacturer, and provider.

Top-Level Root: A Root who is responsible for the governance and administration of its hierarchy, including Roots and CNAs within that hierarchy.

Vulnerability: an instance of one or more weaknesses in a Product that can be exploited, causing a negative impact to confidentiality, integrity, or availability; a set of conditions or behaviors that allows the violation of an explicit or implicit security policy.