***CVE Definitions for CNAs***

These definitions will give CNAs an understanding of terms that are used throughout the CVE Program. Whenever anyone within the CVE Program uses these terms in the context of CVE operations, CNAs should interpret the meanings of those terms based on these definitions.

|  |  |  |
| --- | --- | --- |
| Term | Definition | Synonyms |
| Abstraction |  |  |
| Access Vector | How a vulnerability may be exploited. Examples include a local exploit (by having a presence on the system), a physical exploit (by having physical access to the system), or a network-based exploit (where the vulnerability can be exploited through a network connection). | Extent |
| Attack Vector |  |  |
| Extent | How a vulnerability may be exploited. Examples include a local exploit (by having a presence on the system), a physical exploit (by having physical access to the system), or a network-based exploit (where the vulnerability can be exploited through a network connection). | Access vector |
| Bug | The flaw or design oversight leading to a potential vulnerability. |  |
| Candidate | DEPRICATED |  |
| Codebase | A software component that is shared among multiple products. |  |
| Component | The location in the code that contains the vulnerability. This includes functions, files, plugins, and other possible sub-components of the product. Components tend to be strong indicators of duplicates. |  |
| Configuration Issue | An issue where a purposeful customization in the behavior of software results in an unintended state. |  |
| CNA | CVE Numbering Authority. Organizations that assign and publish CVE IDs for vulnerabilities that will be made public in accordance with CNA Rules. |  |
| CNA Block | Pool of CVE IDs provided to a CNA by MITRE, for the CNA to assign. |  |
| CNA Rules | Administrative rules which maintain consistency in the CVE assignment  process and administration of the CNA program across all CNAs. |  |
| Counting Rules | The rules used for determining the number of unique identifiers to assign relevant to a set of vulnerability disclosures. |  |
| CVE Working Group | A group through which CNAs, the CVE Board, and others can collaborate to develop technology, process, and policy for the CVE program. |  |
| CVE Board | A collection of individuals representing numerous cybersecurity-related organizations, including commercial security tool vendors, academia, research institutions, government departments and agencies, and other prominent security experts, as well as end-users of vulnerability information that provide critical input regarding the data sources, product coverage, coverage goals, operating structure, and strategic direction of the CVE program. |  |
| CVE Board Member | Individuals from numerous cybersecurity-related organizations including commercial security tool vendors, academia, research institutions, government departments and agencies, and other prominent security experts, as well as end-users of vulnerability information. |  |
| CVE Entry | An item in the CVE List. CVE entries contain the CVE ID, a description of the vulnerability, and references to public disclosure sources. |  |
| CVE ID Syntax | The CVE ID syntax is variable length and includes:  CVE prefix + Year + Arbitrary Digits |  |
| CVE IDs | Unique, common identifiers for publicly known cyber security vulnerabilities. |  |
| CVE Identifier | http://cve.mitre.org/find/search\_tips.html#how\_to\_read |  |
| CVE List | A collection of common names (CVE IDs) for publicly known cybersecurity vulnerabilities. |  |
| CVE Program | A program whose primary purpose is to uniquely identify vulnerabilities and to associate specific versions of code bases (e.g., software and shared libraries) to those vulnerabilities. The use of CVE IDs ensures that two or more parties can confidently refer to a unique identifier when discussing or sharing information about a unique vulnerability. |  |
| CVE Request Web Form | Online form used to contact MITRE to request a CVE ID or a block of CVE IDs, request an update to a CVE, provide notification about a vulnerability publication, or submit comments. |  |
| CVE-Compatible | Tool, service, web site, database, or advisory / alert that uses CVE IDs in a way that allows it to cross-link with other repositories that use CVE IDs; reviewed and registered as "CVE-Compatible." |  |
| Duplicate | The creation of a new CVE for an issue that already has one. |  |
| Executable file | A file that causes a computer to perform tasks according to encoded instructions, as opposed to a data file that must be parsed by a program to be meaningful. |  |
| Impact | The type of action that the attacker can trick the software into doing; or, the type of action that the attacker can perform after the software has made a mistake. |  |
| Independently Fixable Vulnerability | A vulnerability that can be removed from the code such that the change does not fix any other reported vulnerabilities. |  |
| Pre-publication | An issue that has not yet been publicly published. | Privately Known |
| Primary CNA | Organization that 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 CVEs assigned at the Sub- or Root CNA levels. |  |
| Privately Known | An issue that has not yet been publicly published. | Pre-publication |
| Problem Type | A combination of attack model (e.g., symlink attack) and the type of mistake that causes the vulnerability (e.g., the product does not properly check permissions). |  |
| Publicly Available | A product that anyone can purchase or obtain legitimate access to. This includes freeware, shareware, open source, and commercial products. |  |
| Publicly Known | An issue that has been published or divulged publicly or is scheduled to be published by a researcher or vendor who has been in communication with the CVE Team regarding the issue).. |  |
| Reference | A link to publicly known information about a vulnerability. Each reference used in CVE has the following structure:  SOURCE: NAME |  |
| Repository | An implicit or explicit collection of security elements that supports a capability, e.g., a vulnerability database, advisory archive, the set of signatures in an intrusion detection system (IDS), or web site. | Git Repository |
| Requester | Someone who requests a CVE ID from a CNA. |  |
| Root CNA | Organization that manages 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. |  |
| Scope | A given CNA’s products or domain of responsibility. |  |
| Software | Programs and other operating information used by a computer ro computer system. talking about everything from a word processor to a IoT device. |  |
| Software Package | A collection of separate, self-contained software components that are distributed as a single, monolithic object. |  |
| Software Product | A collection of installable software distributed under a unique name by a particular vendor or development project. |  |
| Software Version | A unique name for a particular revision of computer software. This includes commit IDs and other versioning identifiers. Within the CVE process, the specific version or versions affected by a vulnerability are key factors in the counting process. |  |
| Source | Discloser of vulnerability information. Associated with a vendor or primary maintainer of a product or set of products; or vulnerability databases, mailing lists, and advisories from coordination centers, which tend to disclose vulnerability information from many different vendors. |  |
| Sub-CNA | Organization that assigns CVEs for vulnerabilities in their scope, and operate under the management of Root CNAs. |  |
| U.S. Information Technology (IT) Sector | A sector defined by a set of functions performed by the entities that comprise it. Those functions provide: a) IT products and services; b) incident management capabilities; c) domain name resolution services; d) identity management and associated trust support services; e) Internet-based content, information, and communications services; and f) Internet routing, access, and connection services. |  |
| Vulnerability | A weakness in the computational logic (e.g., code) found in software and some hardware components (e.g., firmware) that, when exploited, results in a negative impact to confidentiality, integrity, OR availability. Mitigation of the vulnerabilities in this context typically involves coding changes, but could also include specification changes or even specification deprecations (e.g., removal of affected protocols or functionality in their entirety).” |  |