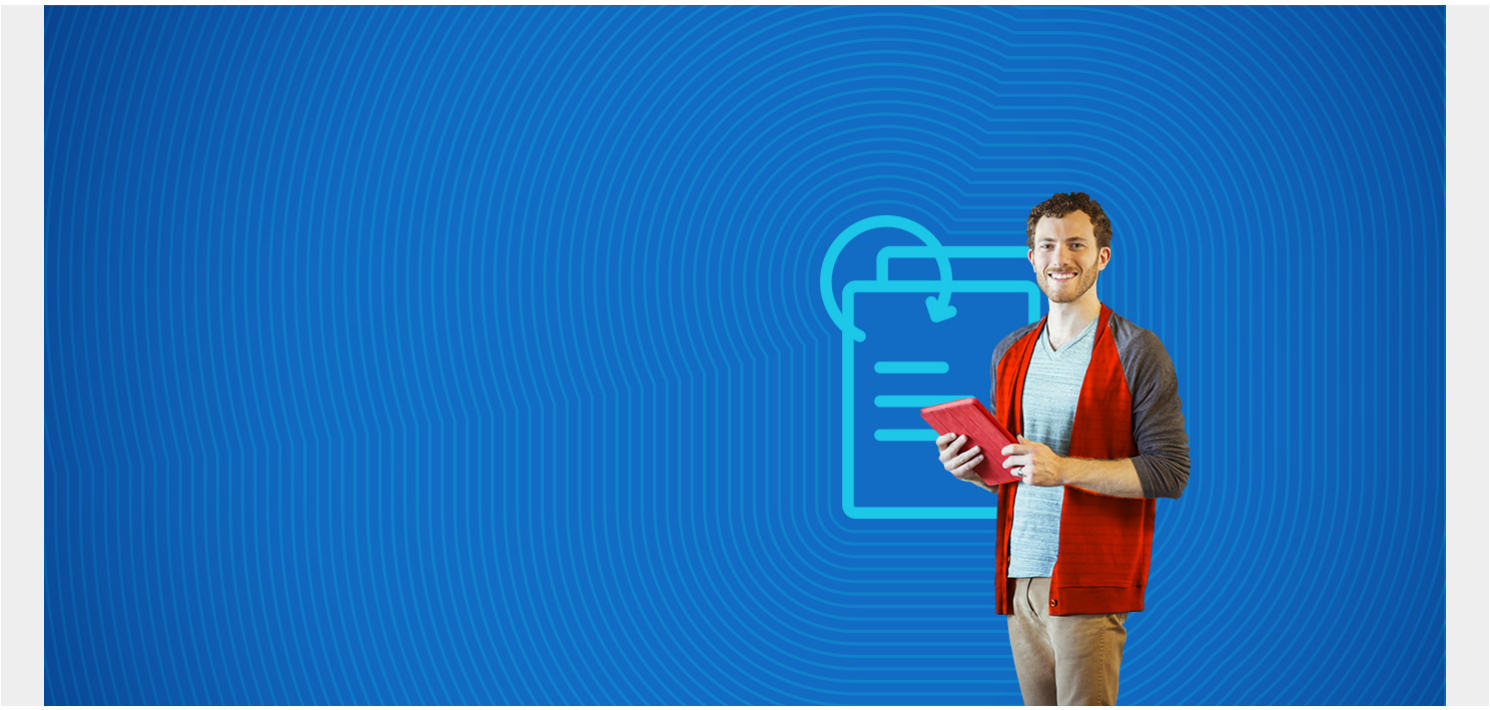
WHAT IS CVE? COMMON VULNERABILITIES AND EXPOSURES EXPLAINED



Common Vulnerabilities and Exposures, often known simply as CVE, is a list of publicly disclosed computer system security flaws. CVE is a public resource that is free for download and use. This list helps IT teams prioritize their security efforts, share information, and proactively address areas of exposure or vulnerability. Doing so makes systems and networks more secure and helps to prevent damaging cyberattacks. A basic understanding of the CVE Project and overview of how CVE works can help organizations better take advantage of and to contribute to this resource.

The Background of CVE

CVE was created in 1999 at a time when most cybersecurity tools used their own databases and their own names for vulnerabilities. Because the available products varied so widely, it was hard to figure out when different databases were referring to the same issue. This led to gaps in security coverage, making it hard to create any good system for interoperability between different databases and tools.

To address these issues, the CVE was developed to provide common, standardized identification. As such, it addressed these underlying concerns and made it possible for IT professionals to share information about vulnerabilities, working together to identify and address those issues. As a result, it's become the industry standard for identifying vulnerabilities and exposures, and it's endorsed by the CVE Numbering Authority, CVE Board, and many industry-leading products and services.

At its core, CVE provides reference points so that different products and services can communicate. This leads to interoperability and better security coverage. Further, it creates a basis for evaluating

services, tools, and databases.

The CVE is maintained by the MITRE Corporation, a non-profit organization that manages federally funded research and development centers supporting U.S. government agencies. MITRE is responsible for maintaining the CVE dictionary and public website. This project is funded by the Department of Homeland Security's Cybersecurity and Infrastructure Agency.

Who Leads CVE Efforts

Much of the success of the CVE Project's efforts has come from the fact that it has been a collaborative effort by the international cybersecurity community. This has enabled the list to be comprehensive, which, in turn, has led to more people using services and products that are compatible with CVE. The key players making contributions to the CVE are the CVE Numbering Authority, the CVE Board, and the CVE Sponsor.

The CVE Numbering Authority (CNA) assigns CVE identification numbers. CNAs are given a block of CVE numbers to hold in reserve and to assign as issues are discovered. There are generally about 100 CNA, and this group includes vulnerability researchers; vendors and projects; national and industry CERTS; and bug bounty programs.

The CVE Board is tasked with ensuring that the CVE Program meets the global cybersecurity community's vulnerability identification needs. It oversees the CVE, provides input about the CVE strategic direction, and advocates on behalf of the CVE. The CVE Board includes cyber-security organizations, commercial security tool vendors, members of academia and research institutions, members of government departments and agencies, and security experts.

The SVE Sponsor is the United States Department of Homeland Security Cybersecurity and Infrastructure Security Agency. CISA is responsible for the funding of the CVE Project.

The Basics of CVE

CVE consists of a list of entries, each of which has an identification number, a description, and a public reference. Each CVE lists a specific vulnerability or exposure. Per the CVE site, a vulnerability is defined as a mistake in software code that gives attackers direct access to a system or network. This type of access allows an attacker to become a super-user or system administrator with full privileges. In contrast, an exposure is a mistake that gives an attacker indirect access to a system or network. This type of access allows an attacker to collect customer information to sell.

Broadly speaking, the CVE Project creates a system for identifying and organizing vulnerabilities and exposures. The first step for creating a CVE listing is identifying a vulnerability or exposure. Next, the vulnerability will be assigned a CVE identification number by the CNA. The CNA then writes a description of the issue and provides references. Finally, the completed CVE entry is added to the CVE list and posted to the CVE website.

CVE offers a single, unique identifier for each specific exposure or vulnerability. It's worth noting that it's more like a dictionary than a database. The description for each entry is brief and does not include technical data, information about specific impacts, or information about fixes. Instead, that information is found in other databases, for example, the U.S. National Vulnerability Database (NVD) or CERT/CC Vulnerability Notes Database.

CVE Identifiers

When referring to CVE, people usually refer to a specific identification number. These common identifiers, referred to as CVEs, CVE IDs, or CVE numbers, allow for consistency when discussing or sharing information about specific vulnerabilities. CVE identifiers can be issued by CNAs or directly by MITRE. Thousands of CVE IDs are assigned each year, and a single complex project, like an operating system, can have hundreds of CVEs.

Vulnerabilities or exposures in need of a CVE identifier can be identified by anyone - a researcher, vendor, or even a savvy user. In fact, to encourage the disclosure of flaws, some vendors even offer "bug bounties." That said, not all flaws are assigned a CVE. To be assigned a CVE ID, the issue must be:

- Independently fixable, meaning that it can be resolved independently of other bugs
- Acknowledged by the software or hardware vendor OR documented with a vulnerability report
- Affecting only one codebase. If a flaw is affecting more than one product, each is given its own CVE ID.

It's worth noting that, to ensure that information in the CVE list is not exploited by cyberattackers, sometimes a CVE will be assigned before a public security advisory is issued. To reduce the risk of attacks once a vulnerability is identified, they are often kept secret until a fix has been developed and tested.

Next Steps

The CVE Project is a great resource for all IT organizations to use. It's especially important for researchers and product developers to utilize CVE entries and to use products and services that are compatible with CVE. Additionally, it's important to always be looking for vulnerabilities in software and to share any that your organization finds when using open-source software. Further, it's key to communicate about vulnerabilities internally and externally to help prevent attacks and to efficiently resolve issues.

While CVE entries are a great resource, it's key to analyze all entries that apply to products your organization uses. Not all issues apply in all situations, and whenever they are applicable, it's necessary to conduct vulnerability management in order to prioritize risks. The Common Vulnerability Scoring System (CVSS) is a popular way to determine how severe a vulnerability is and, subsequently, to prioritize cybersecurity efforts. The CVSS provides open standards to assign a number, or rating, to a vulnerability. These numbers range from 0.0 to 10.0, and the higher the number, the greater the severity. Using the CVSS or a similar system is a key aspect of vulnerability management and can help to effectively focus cybersecurity efforts.