

[Cybersecurity 101: The Fundamentals of Cybersecurity](#) > [Exposure Management In Cybersecurity](#) > [What Is CVE?](#)
[Common Vulnerabilities & Exposures](#)

WHAT IS CVE?

COMMON VULNERABILITIES & EXPOSURES

Arfan Sharif - December 07, 2022

Businesses today are **more at risk** from cybersecurity attacks and data breaches than ever before. Data theft and ransomware attacks from vulnerabilities and exposures **can cause millions of dollars in damages** for corporations.

But what exactly are vulnerabilities and exposures? We can describe a vulnerability as a **fault or weakness within a computer system or software that can grant unintended levels of access to a user**. Vulnerabilities allow attackers to perform destructive actions on a computer system or network, such as installing malware or gaining unauthorized access to information.

An exposure is a **misconfiguration that gives attackers access to a computer system or the data it stores**. One example would be a loosely secured cloud storage system that allows attackers to **access sensitive data**. Another example would be an open network port on a server which is further exploited through the installation of command and control malware.

Another way to think about an exposure is as a vulnerability actively being exploited by attackers.

The applications we use daily are prone to vulnerabilities and exposures due to their complex natures and the short development cycles for each new release. Realizing this, vendors often quickly develop and release patches for vulnerabilities as soon as they are detected. Because of this, developers have felt the need for an effective communication tool regarding recently discovered vulnerabilities. Therefore, we have Common Vulnerabilities and Exposures (CVEs), **an international framework and effort to maintain an updated registry of all known computer security vulnerabilities and exposures**.

In this post, we'll discuss what CVEs are and why they're critical to reporting and publishing vulnerabilities. We'll also learn how to use CVEs and the best tools to keep you updated on the latest security threats.

Let's begin with a basic overview of CVEs.

I An Overview of CVEs: Core Concepts

According to **Deloitte's report**, most companies spend about 10% of their annual IT **budget on cybersecurity**. This is a significant amount of money for medium to large organizations. One way to reduce this cost is to maintain an updated database of known vulnerabilities.

A Central Database Operated by the MITRE Corporation

CVE is operated by the MITRE Corporation and funded in part by the United States Department of Homeland Security. CVEs have

GoSecure, Inc.
Exhibit 2042
CrowdStrike v. GoSecure
IPR2025-00070

vulnerabilities.

A Central Database Operated by the MITRE Corporation

CVE is operated by the MITRE Corporation and funded in part by the United States Department of Homeland Security. CVEs have become an indispensable source of information for cybersecurity professionals worldwide. Developers and organizations rely on CVEs to receive critical security updates, stay informed on breached systems, and implement preventative measures to thwart malicious attacks.

Although MITRE manages a list of current CVEs, they don't actively search for new application vulnerabilities. That task falls on individuals or organizations in the open-source community who spend their time and effort discovering application flaws and reporting them to the vendors.

CVE Numbering Authorities (CNAs)

MITRE Corporation's other role in the CVE program is to manage the CVE Numbering Authorities (CNAs). CNAs are organizations throughout the world that are also CVE program partners. CNAs are usually part of major corporations — such as Microsoft, Oracle or Apple — and they're essentially a bridge between individuals who find a new vulnerability and the CVE community. They help the discovery process by checking and submitting documents about the vulnerability and publishing the CVE.

CNAs are also in charge of assigning unique IDs to new CVEs. The ID helps you find all the relevant information about a vulnerability or exposure. Different CVE databases worldwide use these IDs to add more detailed information about the CVE, including:

- Severity
- Affected software systems
- The steps to follow to patch the vulnerability and contain the damage

Created to Share and to Inform

CVEs were created to share information and technical details about these vulnerabilities with the wider community, informing everyone about the latest threat landscape and instructing them on how to defend against the ever-emerging risks.

Such vulnerabilities can come from unmaintained open-source software and commercial applications alike. Software developers often use third-party libraries and dependencies to develop applications. The greatest benefit of a centralized CVE reporting system is that it can alert everyone at the same time about vulnerable applications or libraries.

Examples of CVEs

A classic example of a CVE is the [recent Log4j vulnerability report](#) (CVE-2021-44228). It contains detailed information about a vulnerability of the popular Java logging framework, Apache Log4j. Many service providers, like AWS, Cloudflare and Twitter, were affected by this vulnerability.

Another example is the ProxyShell vulnerability. It affected Microsoft Exchange servers by allowing remote code execution. It was announced via [CVE-2021-34473](#), [CVE-2021-34523](#) and [CVE-2021-31207](#).

Integrating CVE Scanning into CI/CD

One of the best use cases of CVEs is to include them in your application development and deployment pipeline. As mentioned before, applications may often use packages or libraries with vulnerabilities. By including the CVE scanning capability in the [CI/CD pipeline](#), developers can automate security testing, stop the code from merging into the code repository and receive alerts.

Integrating CVE Scanning into CI/CD

One of the best use cases of CVEs is to include them in your application development and deployment pipeline. As mentioned before, applications may often use packages or libraries with vulnerabilities. By including the CVE scanning capability in the **CI/CD pipeline**, developers can automate security testing, stop the code from merging into the code repository and receive alerts.

What Qualifies as a CVE?

Before a CVE can be accepted and published, it must meet a specific set of criteria. Fulfilling the requirements helps separate and distinguish between bugs and vulnerabilities. As a CNA, you don't want to go through countless CVE reports only to find out most of them are bugs that developers can fix by changing a few lines of code. The following are some of the criteria for qualifying as a CVE.

Repairability

The vulnerability should be repairable. This means that the end user should be able to resolve the problem by installing a software update that includes a patch for that vulnerability.

Provability

The entity filing the report must be able to prove the alleged vulnerability through documentation or present the software vendor's confirmation.

Limited Effect

The vulnerability should affect only a single piece of software or codebase. If the vulnerability affects multiple products, it should be split into different CVEs.

It's worth noting that even if a vulnerability fulfills all of these criteria, it may not be published immediately. Delaying publication can give the vendor time to develop a patch. This allows the vendor to announce the fix at the same time the CVE is made public.

Many companies also offer **bug bounty programs** to encourage the community to discover and report vulnerabilities. Bug bounty hunters are experienced cybersecurity professionals who perform extensive tests to identify threats and exposures in an application.

What Is the Common Vulnerability Scoring System (CVSS)?

CVEs can be of different types with varying levels of severity and needing varying degrees of attention. Since CVEs are being published all the time, the Common Vulnerability Scoring System (CVSS) helps determine how to prioritize CVEs.

CVSS is a numbering system for assigning priority and severity levels to CVEs. It works by assigning a number between 0.0 and 10.0 to a CVE, indicating its severity. A vulnerability with a CVSS score between 9.0 and 10.0 is considered critical and needs immediate action.

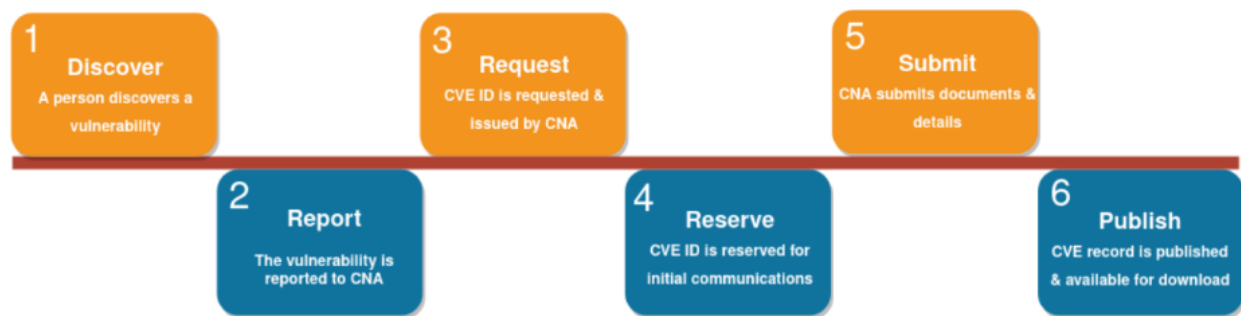
CVSS helps companies plan **risk management** and response strategies and prioritize their patching cycles. Many security advisories release lists of CVEs ordered by the CVSS scores, with more severe vulnerabilities at the top of the list.

How Does CVE Work?

When a vulnerability is discovered, it must go through a standardized CVE lifecycle before publication. The image below shows a simplified flow.

I How Does CVE Work?

When a vulnerability is discovered, it must go through a standardized CVE lifecycle before publication. The image below shows a simplified flow.



Discover: The process starts with a person or organization discovering a vulnerability.

Report: The person or entity that discovered the vulnerability files a report with a CVE program partner.

Request: The CVE partner (CNA) issues an ID for the vulnerability.

Reserve: The ID is reserved for that particular vulnerability and is used in the early-stage assessment of the CVE and all related communications between different parties.

Submit: The CVE partner assesses the vulnerability's submitted documents, which should include all information needed to prove the presence of the vulnerability or exposure, the root cause, the type of threat and the impact.

Publish: After all the documented details are verified, the CNA publishes the CVE, making it public.

I Challenges of Staying Informed on the Latest CVEs

CVEs offer valuable information about the latest computer system vulnerabilities. However, there are too many to sort through every week, and not all CVEs may apply to your organization's landscape. These announcements are only effective if you can stay updated.

The United States Computer Emergency Readiness Team (**US-CERT**) is one of the organizations providing public security **advisory services** on CVEs. They send a weekly newsletter containing the latest CVEs ordered by severity. If you're trying to stay informed, another option is to subscribe to the RSS feed of the **CERT/CC Vulnerability Notes Database** to receive real-time notifications.

Vulnerability management platforms can increase the effectiveness of your organization's IT security initiatives. These platforms constantly assess, research, and report active vulnerabilities within your infrastructure and applications. The graphical dashboards help you get a bird's-eye view of the current threat posture, track vulnerabilities and receive step-by-step patching information.

I CVE Solutions

CVEs play a major role in disseminating information about new vulnerabilities and are vital for an organization's fight against security threats.

Unified threat and vulnerability management platforms like CrowdStrike help you research CVEs and analyze threat actor profiles in a timely manner. **CrowdStrike Falcon® Spotlight** offers real-time threat analysis for your IT infrastructure and applications. To

CVEs play a major role in disseminating information about new vulnerabilities and are vital for an organization's fight against security threats.

Unified threat and vulnerability management platforms like CrowdStrike help you research CVEs and analyze threat actor profiles in a timely manner. **CrowdStrike Falcon® Spotlight** offers real-time threat analysis for your IT infrastructure and applications. To learn more, [start your free trial](#).



Arfan Sharif is a product marketing lead for the Observability portfolio at CrowdStrike. He has over 15 years experience driving Log Management, ITOps, Observability, Security and CX solutions for companies such as Splunk, Genesys and Quest Software. Arfan graduated in Computer Science at Bucks and Chilterns University and has a career spanning across Product Marketing and Sales Engineering.

Featured Articles

What is a Cyberattack?



Cyberattacks

Cloud Infrastructure Entitlement Management (CIEM)



Cloud Infrastructure Entitlement Management (CIEM)

What is Centralized Logging?



Centralized Logging

Try CrowdStrike free for 15 days

[Start free trial →](#)

[Contact us →](#)

[View pricing >](#)



Cyberattacks



Cloud Infrastructure Entitlement Management (CIEM)



Centralized Logging

Try CrowdStrike free for 15 days

Start free trial →

Contact us →

View pricing >



Get Started	Company	Partners	Existing Customers	Support
Pricing Sale	About Us	Partner Programs	Support Portal	Call 1-888-512-8906 (US)
Free Trial Guide	Executive Leadership	Service Providers	Developer Portal	Experienced a Breach?
Falcon Flex	Board of Directors	Strategic Technology		Contact Us
Financing	Newsroom	Channel & Distributors		Schedule a Meeting
CrowdStrike Marketplace	Investor Relations	Become a Partner		FAQs
Cyber Monday Deals	CrowdStrike Racing & F1			
	Sustainability			