What are CVEs?

By DarkOwl Content Team

Published: 2024-05-14 · Archived: 2026-04-05 14:55:02 UTC

May 14, 2024

Cybersecurity might has well have its own language. There are so many acronyms, terms, sayings that cybersecurity professionals and threat actors both use that unless you are deeply knowledgeable, have experience in the security field or have a keen interest, one may not know. Understanding what these acronyms and terms mean is the first step to developing a thorough understanding of cybersecurity and in turn better protecting yourself, clients, and employees.

In this blog series, we aim to explain and simplify some of the most commonly used terms. In this edition, let's dive into CVEs.

CVEs 101

CVE is an acronym thrown around frequently in the cybersecurity space. CVE stands for Common Vulnerabilities and Exposures. A CVE is a list of publicly disclosed cybersecurity vulnerabilities that are assigned a unique identifier called a CVE ID. According to the National Institute of Standards and Technology, CVE defines a vulnerability as "a weakness in the computational logic (e.g., code) found in software and hardware components 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)." When a security vulnerability is identified, it receives a CVE ID number. This identifier is used to monitor and reference the vulnerability in security advisories released by vendors and researchers, and have a uniform way in searching the same vulnerability across databases.

The concept of the CVE database originated in a whitepaper by co-creators Steven M. Christey and David E. Mann of the MITRE Corporation. The initial CVE list was publicly available in 1999, and continues to grow. There are currently over 247,000 CVEs and in the first week of 2024 alone, over 600 were cataloged. The system is maintained by the United States' National Cybersecurity FFRDC, which is run by the MITRE Corporation and receives finding from the US Department of Homeland Security's National Cyber Division.

Keeping a record of all CVEs allows security and IT researchers to coordinate efforts in prioritizing and resolving these vulnerabilities. To keep CVE records organized, there is a CVE Program dedicated to identifying, defining, and cataloging publicly disclosed cybersecurity vulnerabilities.

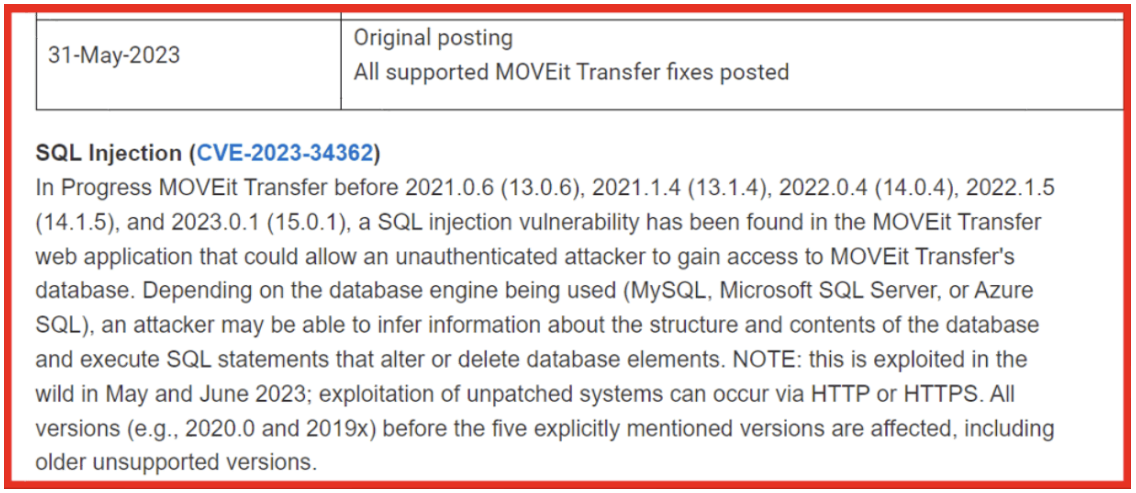
Not only are CVEs important for keeping track of vulnerabilities in a way that is repeatable, searchable and trackable, but they raise security awareness. Because CVEs are publicly documented, there is better awareness of potential threats and security concerns. Individuals and organizations have the ability to search vulnerabilities and

take the necessary actions to secure their computer systems and networks. CVEs allow security professionals to stay up to date on the latest security flaws and vulnerabilities.

CVEs in the Wild

CVE-2023-34362: MOVEit Transfer

In 2019, the Cl0p ransomware gang shifted their focus to exploiting the MOVEit vulnerability to target victims starting in May 2023, and they carried on with this campaign throughout the summer. They exploited the SQL injection vulnerability known as CVE-2023-34362 in the MOVEit transfer system, which is extensively utilized for managing file transfer operations across numerous organizations. Cl0p's exploitation of this vulnerability had significant repercussions for several prominent brands and companies, garnering substantial media coverage. It's estimated that roughly 2,000 instances of the MOVEit vulnerability were exploited, affecting approximately 60 million individuals worldwide. These figures may be conservative due to under-reported incidents and efforts by affected entities to conceal the extent of network intrusions. Nevertheless, experts projected that the group stood to gain around $100 million from exploiting this vulnerability. If this vulnerability were to be left unaddressed, it could lead to significant data breaches, loss of sensitive information, and severe disruption of services.



31-May-2023	Original posting All supported MOVEit Transfer fixes posted

SQL Injection (CVE-2023-34362)
In Progress MOVEit Transfer before 2021.0.6 (13.0.6), 2021.1.4 (13.1.4), 2022.0.4 (14.0.4), 2022.1.5 (14.1.5), and 2023.0.1 (15.0.1), a SQL injection vulnerability has been found in the MOVEit Transfer web application that could allow an unauthenticated attacker to gain access to MOVEit Transfer's database. Depending on the database engine being used (MySQL, Microsoft SQL Server, or Azure SQL), an attacker may be able to infer information about the structure and contents of the database and execute SQL statements that alter or delete database elements. NOTE: this is exploited in the wild in May and June 2023; exploitation of unpatched systems can occur via HTTP or HTTPS. All versions (e.g., 2020.0 and 2019x) before the five explicitly mentioned versions are affected, including older unsupported versions.

CVE-2023-22515: Confluence Data Center and Server by Atlassian

Last fall, the Ukrainian Cyber Alliance (UCA) used CVE-2023-22515, which involves Confluence, to escalate privileges and access Trigona's confluence server. They gained insight into the infrastructure and published Trigona's support documents, exfilled the developer environment and information pertaining to Trigona's crypto payments, as well as the back-end of Trigona's chat service and blog/leak site details. After collecting all the information, UCA defaced and deleted Trigona's site. Open CVE's provide danger to all, including the cybercriminals who use the impacted tools.

CVE-2022-42475: FortiOS SSL-VPN Vulnerability

Continuing their world-wide efforts to infiltrate government, military, and key sources of intel, China exploited an extant Fortinet vulnerability (CVE-2022-42475) in early February of this year. This was done to deploy a backdoor named COATHANGER and gain access to a network used by the Dutch military. This was the first time

the Dutch have publicly attributed a cyber incident to Chinese actors. This vulnerability, along with CVE-2023-22515, emphasize the importance of maintaining good security hygiene and always updating computer systems to the latest version.

CVEs in DarkOwl Vision

Cyber Actors Discuss CVEs on the Darknet

Cyber criminals and hackers frequently discuss vulnerabilities on the darknet for various platforms. Discussions of relevant software and exploitability of specific CVEs can assist an organization in determining potential unpatched vulnerabilities. Figure 2 shows a forum discussion about an exploit for CVE-2022-30190, which is a Microsoft office vulnerability that hackers can leverage for remote code execution.

Figure 2: DarkOwl Vision search reveals an exploit based on CVE-2022-30190; Source: DarkOwl Vision

Figure 3 shows a post to a hacker forum on the darknet by the user known by the moniker, PresidentXS, that discusses an Azure vulnerability, CVE-2019-1306, “Azure DevOps and Team Foundation Server Remote Code

Execution Vulnerability.” An attacker successfully exploiting this vulnerability allows for malicious code execution on an ADO service account.

Figure 3: Source: DarkOwl Vision

Posts and discussion threads like these examples in DarkOwl Vision are useful for reviewing comments, exploring applications, and use cases for the vulnerability specifically.

Tokenization

Based on feedback from our customers, CVEs are identified and tokenized within our indexed documentation collection. DarkOwl Vision UI users can search for results containing a specific CVE number, as well as for results containing any number of CVEs. CVE tokenization makes it easier to search for CVEs along side keywords or other entities such as onion domains or threat actor aliases.

Figure 4: CVE search in Vision UI; Source: DarkOwl Vision

Actor Explore

DarkOwl's Actor Explore feature provides invaluable insights into cyber threat actors, empowering security professionals, researchers, and organizations with analyst curated information about threat actors, enhancing their ability to understand and combat cybersecurity threats effectively. Each actor profile in Actor Explore includes a detailed dossier, offering an in-depth overview of the threat actor and includes extensive information such as darknet fingerprints, targets, tools, CVEs, contact information, and more. Actor Explore connects this information to our other data sets, including leak sites, ransomware sites, alias, cryptocurrency, etcetera that actors are associated with. This wealth of data enables users to gain a profound understanding of the threat actors, their tactics, and the potential risks they pose.

A DarkOwl Vision user can also search in Actor Explore by CVE. This filtering option makes it easier to find and compare actors of interest.

Figure 5: DarkOwl Actor Explore result for Cl0p and the CVEs they exploit; Source: DarkOwl Vision

Figure 6: Example of CVE filtering in Actor Explore; Source: DarkOwl Vision

Resources

Keeping up to date on CVEs is essential to maintaining a secure IT environment. Below are a couple free resources available for tracking and researching CVEs.

- CVE Program Mission: Identify, define, and catalog publicly disclosed cybersecurity vulnerabilities. View the 228,713 CVE records available.
- CVE Tracker: A New Motional Open-Source Tool for Tracking Common Vulnerabilities and Exposures. View tool here.

To take investigations the next step, root cause mapping of vulnerabilities is best done by correlating CVE Records. Check out guidance from Mitre here.

To see DarkOwl Vision and our collection of CVEs in action, contact us.
