

Lab - Investigate Vulnerability Information Sources

Objectives

Use multiple helpful sources to further investigate vulnerabilities.

- Part 1: Investigate Common Vulnerabilities and Exposures (CVEs)
- Part 2: Explore Common Weakness Enumerations (CWEs)
- Part 3: Investigate National Institute of Standards and Technology (NIST) Vulnerability Resources
- Part 4: Research Vulnerabilities in the Common Vulnerability Scoring System (CVSS)

Background / Scenario

In a previous lab, you found several vulnerabilities after scanning a target system. You will now use several widely available sources to dig deeper into the details of the vulnerabilities. You will map and investigate the vulnerabilities to the Common Vulnerabilities and Exposures (CVE) list, the Common Weakness Enumeration (CWE), the NIST National Vulnerability Database, and the Common Vulnerability Scoring System (CVSS).

Required Resources

- Computer with internet connection

Instructions

Part 1: Investigate Common Vulnerabilities and Exposures (CVEs)

Step 1: Explore CVE.

- Launch the CVE website and navigate to www.cve.org.
- Read the overview of the CVE program.

Screenshot of the CVE (Common Vulnerabilities and Exposures) website homepage.

The page features a search bar at the top with the placeholder "Enter keywords (e.g.: CVE ID, sql injection, etc.)" and a "Search" button. Below the search bar is a notice about expanded keyword searching. The main header is "CVE™ Program Mission". A sub-header below it reads: "Identify, define, and catalog publicly disclosed cybersecurity vulnerabilities." A note states: "There are currently over 308,000 CVE Records accessible via [Download](#) or [Keyword Search](#) above."

A central callout box contains text about the CVE Program partners and the role of CVE Numbering Authorities (CNAs). It includes two buttons: "Learn More" and "Become a Partner". To the right is a circular graphic showing a network of users connected to a central "CVE" node.

Below this are three sections: "Access", "Learn", and "Report/Request".

- Access:**
 - List of Partners
 - CNA Rules
 - CVE Record Lifecycle
 - CVEProject on GitHub for Development
 - CVE Record User Guide
- Learn:**
 - About CVE
 - Process
 - Program Organization
 - Related Efforts
 - Terminology
 - CVE Services for CNAs
- Report/Request:**
 - Report vulnerability/Request CVE ID
 - Request CVE Record be published/updated
 - Report the use of a reserved CVE ID

A banner below these sections says "Access Resources Based on Role".

The right sidebar is titled "News" and lists several recent articles:

- CVE Record Disputes, Explained: A Community Path to Clearer Vulnerability Data in a Compliance-Driven World
- FINAL WEEK! — Call for Speakers for VulnCon 2026 Closes on December 22, 2025
- "Vulnogram User Guide" for CNAs Updated
- Minutes from CVE Board Teleconference Meeting on November 12 Now Available
- runZero, Inc. Added as CVE Numbering Authority (CNA)
- Vulnerability Data Enrichment for CVE Records: 256 CNAs on the Enrichment Recognition List for December 1, 2025

NEWS ICONS

1. Select About > Overview in the menu.

Screenshot of the CVE website showing the "About > Overview" page.

The page has a similar header and search bar as the homepage. The main content area is titled "Overview".

On the left, there's a section titled "About the CVE Program" with text explaining the mission of the program. Below this is a video player for a "CVE Lightning Talk".

On the right, there's a sidebar titled "About" with a "Overview" tab selected. Other tabs include "About The CVE Program", "History", "Process", "Related Efforts", and "Metrics".

- View the CVE Program Overview video.
- Review the available Podcasts for more detailed information about the CVE program

What is the mission of the CVE program?

Answer Area

to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities.

Show Answer

Who assigns CVE IDs?

Answer Area

CNAs(CVE Numbering Authorities)

Show Answer

What are the two main goals of the CVE Program?

Answer Area

produce more CVE records faster
scale the program for broader adoption and coverage

Show Answer

Who operates the CVE?

Answer Area

MITRE Corporation with funding from the US Department of Homeland Security (DHS) and the Cybersecurity and Infrastructure Security Agency (CISA) Vulnerability Management

Show Answer

Step 2: Use the CVE program to gather information about vulnerabilities.

In an earlier lab, you scanned a target system for vulnerabilities. The list of vulnerabilities found returned the following six CVEs:

- CVE-2021-41617
- CVE-2020-14145
- CVE-2019-16905
- CVE-2019-6111
- CVE-2019-6110
- CVE-2019-6109

a. Enter **CVE-2021-41617** info the search window and click **Find**.

CVE-2021-41617 PUBLISHED

Description
sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

Product Status
Information not provided

References 14 Total

- <https://www.openssh.com/security.html>
- <https://www.openwall.com/lists/oss-security/2021/09/26/1>
- <https://www.openssh.com/txt/release-8.8>

What versions of OpenSSH are subject to this vulnerability?

Answer Area

OpenSSH 6.2 through 8.x before 8.8

Show Answer

When was this CVE last updated?

Answer Area

2023-12-26

Show Answer

At the bottom of the page click **CVE-2021-41617** to view additional information about the CVE from the NIST National Vulnerability Database (NVD).

The screenshot shows the NIST National Vulnerability Database interface. At the top, there's a blue header bar with the text "Information Technology Laboratory" and "NATIONAL VULNERABILITY DATABASE". To the right is the NIST logo and the text "NATIONAL VULNERABILITY DATABASE NVD". Below the header, there's a green button labeled "VULNERABILITIES". The main content area has a white background. On the left, under the heading "MODIFIED", it says "This CVE record has been updated after NVD enrichment efforts were completed. Enrichment data supplied by the NVD may require amendment due to these changes." Under "Description", it states: "sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user." On the right, under "QUICK INFO", it lists: "CVE Dictionary Entry: CVE-2021-41617", "NVD Published Date: 09/26/2021", "NVD Last Modified: 11/21/2024", and "Source: MITRE". Below these, there's a section titled "Metrics" with three buttons: "CVSS Version 4.0", "CVSS Version 3.x", and "CVSS Version 2.0". A note below says "NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed." It also shows "CVSS 3.x Severity and Vector Strings: NVD: NIST: NVD" and "Base Score: 7.0 HIGH" with a corresponding vector string: "CVSS:3.1/A:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H".

What is the CVSS 3.x Severity score for this CVE?

Answer Area

7.0 High

Repeat steps a and b. to review information for the other five CVEs.

The screenshot shows the CVE-2019-6111 page on the cve.org website. The page title is "CVE-2019-6111 PUBLISHED". The main content area is titled "Required CVE Record Information" and contains the following sections:

- CNA:** MITRE Corporation
- Published:** 2019-01-31 **Updated:** 2022-12-13
- Description:** An issue was discovered in OpenSSH 7.9. Due to the scp implementation being derived from 1983 rcp, the server chooses which files/directories are sent to the client. However, the scp client only performs cursory validation of the object name returned (only directory traversal attacks are prevented). A malicious scp server (or Man-in-The-Middle attacker) can overwrite arbitrary files in the scp client target directory. If recursive operation (-r) is performed, the server can manipulate subdirectories as well (for example, to overwrite the .ssh/authorized_keys file).
- Product Status:** Learn more. Information not provided.
- References:** 23 Total
 - [debian.org: DSA-4387](#) vendor-advisory
 - <https://security.netapp.com/advisory/ntap-20190213-0001/>

The right sidebar is titled "On This Page" and lists:

- Required CVE Record Information
- CNA: MITRE Corporation
- CVE Program
- Authorized Data Publishers
- CISA-ADP

Which of these CVEs involves Man-in-the-Middle attacks from a malicious SCP server?

Answer Area

CVE-2019-6111

On the CVE site (www.cve.org), enter **CVE-2019-6111** into the search box and click **Find**.

- Scroll down to the bottom of the CVE page and click **CVE-2019-6111** to view additional information on the NVD.
- On the NVD page for **CVE-2019-6111**, scroll down to the **Weakness Enumeration** section.

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-190	Integer Overflow or Wraparound	NIST

Known Affected Software Configurations Switch to CPE 2.2

Configuration 1 (hide)

cpe:2.3:a:openbsd:openssl:.*:.*:.*:.*:*	From (including)	Up to (including)
<small>Show Matching CPE(s)▼</small>	7.7	7.9
cpe:2.3:a:openbsd:openssl:.*:.*:.*:.*:*	From (including)	Up to (excluding)
<small>Show Matching CPE(s)▼</small>	8.0	8.1

Configuration 2 (hide)

cpe:2.3:a:netapp:cloud_backup:.*:.*:.*:.*:*	From (including)	Up to (including)
<small>Show Matching CPE(s)▼</small>	7.7	7.9
cpe:2.3:a:netapp:steelstore_cloud_integrated_storage:.*:.*:.*:.*:*	From (including)	Up to (excluding)
<small>Show Matching CPE(s)▼</small>	8.0	8.1

Configuration 3 (hide)

cpe:2.3:o:siemens:scalance_x204rna_firmware:.*:.*:.*:.*:*	Up to (excluding)
<small>Show Matching CPE(s)▼</small>	3.2.7

Running on/with

cpe:2.3:h:siemens:scalance_x204rna:.*:.*:.*:.*:*	Up to (excluding)
<small>Show Matching CPE(s)▼</small>	3.2.7

Configuration 4 (hide)

cpe:2.3:o:siemens:scalance_x204rna_ecc_firmware:.*:.*:.*:.*:*	Up to (excluding)
<small>Show Matching CPE(s)▼</small>	3.2.7

Running on/with

Part 2: Explore Common Weakness Enumeration (CWE)

Step 1: Explore CWE.

- Launch the CWE website and navigate to <https://cwe.mitre.org>.
- Explore the CVE program by selecting **About > Overview** in the menu.

What is the goal of CWE? **To stop vulnerabilities at the source by educating software and hardware architects, designers, programmers, and acquirers on how to eliminate common mistakes before products are delivered.**

What is the difference between a CVE and a CWE? **CVE identify, define, and catalog publicly disclosed cybersecurity vulnerabilities while CWE lists common software and hardware weaknesses.**

IDs you recorded from Part 1 step 2.

- Enter 22 in the **ID Lookup** box on the top right of the CWE page. (This is the CWE ID for CVE-2019-6111), What is title of this CWE?

CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

The product uses external input to construct a pathname that is intended to identify a file or directory that is located underneath a restricted parent directory, but the product does not properly neutralize special elements within the pathname that can cause the pathname to resolve to a location that is outside of the restricted directory.

Description

Many file operations are intended to take place within a restricted directory. By using special elements such as ".." and "/" separators, attackers can escape outside of the restricted location to access files or directories that are elsewhere on the system. One of the most common special elements is the "../" sequence, which in most modern operating systems is interpreted as the parent directory of the current location. This is referred to as relative path traversal. Path traversal also covers the use of absolute pathnames such as "/usr/local/bin" to access unexpected files. This is referred to as absolute path traversal.

Alternate Terms

- Directory traversal
- Path traversal

"Path traversal" is preferred over "directory traversal," but both terms are attack-focused.

Repeat step c. Look up the remaining CWE IDs that you recorded in Part 1 Step 2g.

CWE-203: Observable Discrepancy

The product behaves differently or sends different responses under different circumstances in a way that is observable to an unauthorized actor, which exposes security-relevant information about the state of the product, such as whether a particular operation was successful or not.

Discrepancies can take many forms, and variations may be detectable in timing, control flow, communications such as replies or requests, or general behavior. These discrepancies can reveal information about the product's operation or internal state to an unauthorized actor. In some cases, discrepancies can be used by attackers to form a side channel.

Alternate Terms

- Side Channel Attack

Observable Discrepancies are at the root of side channel attacks.

Common Consequences

Impact	Details
Read Application Data; Bypass Protection Mechanism	Scope: Confidentiality, Access Control An attacker can gain access to sensitive information about the system, including authentication information that may allow an attacker to gain access to the system.
Read Application Data	Scope: Confidentiality When cryptographic primitives are vulnerable to side-channel-attacks, this could be used to reveal unencrypted plaintext in the worst case.

Potential Mitigations

Phase(s)	Mitigation
Architecture and Design	Strategy: Separation of Privilege Compartmentalize the system to have "safe" areas where trust boundaries can be unambiguously drawn. Do not allow sensitive data to go outside of the trust boundary and always be careful when interfacing with a compartment outside of the safe area. Ensure that appropriate compartmentalization is built into the system design, and the compartmentalization allows for and reinforces privilege separation functionality. Architects and designers should rely on the principle of least privilege to decide the appropriate time to use evidence and the time to drop evidence.

Part 3: Investigate National Institute of Standards and Technology (NIST) Vulnerability Resources

Step 1: Explore NIST.

- a. Launch the NIST website by navigating to <https://www.nist.gov>.
- b. Select **About NIST > About Us** in the menu and review the overview of NIST.

The screenshot shows a web browser displaying the NIST About Us page. The top navigation bar includes links for OffSec, Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, YouTube, Temp Mail - Disposable..., and Cisco Networking Academy. The main content area features a collage of images related to science and technology. On the left, there is a sidebar with links for About Us, Contact Us, Visit, Careers, Work with NIST, History, and Educational Resources. The main content area has a heading "About NIST" with a brief history of the agency. Below it is a section titled "Mission" with a description of NIST's role in advancing measurement science, standards, and technology. There is also a "Vision" section and a "Core Competencies" section listing Measurement science, Rigorous traceability, and Development and use of standards. A "Share" button on the left allows users to share the page via social media or email. A "Was this page helpful?" button is located in the bottom right corner.

Explore the National Vulnerability Database (NVD).

1. Return to the NIST home page and select **What We Do > Information Technology** in the menu.
2. Select **National Vulnerability Database** in the **Featured Content** list.

The screenshot shows the NIST Information Technology homepage. At the top, there's a banner with a blue circuit board background. Below it, a green bar contains the text "INFORMATION TECHNOLOGY". Underneath, there's a sidebar with links to various NIST programs like the Computer Security Resource Center and the National Vulnerability Database. The main content area features three cards: "Computer Security Resource Center" (with an image of a shield and network nodes), "Cybersecurity Framework" (with a circular diagram showing "RECOV", "GOVERN", "DEFEND", "DETECT", and "PROJECT"), and "National Vulnerability Database" (with an image of a shield and a checkmark). A text box below the cards states: "Advancing the state-of-the-art in IT in such applications as cyber security and biometrics, NIST accelerates the development and deployment of systems that are reliable, usable, interoperable, and secure; advances measurement science through innovations in mathematics, statistics, and computer science; and conducts research to develop the measurements and standards infrastructure for emerging information technologies and applications." A "Was this page helpful?" link is at the bottom right.

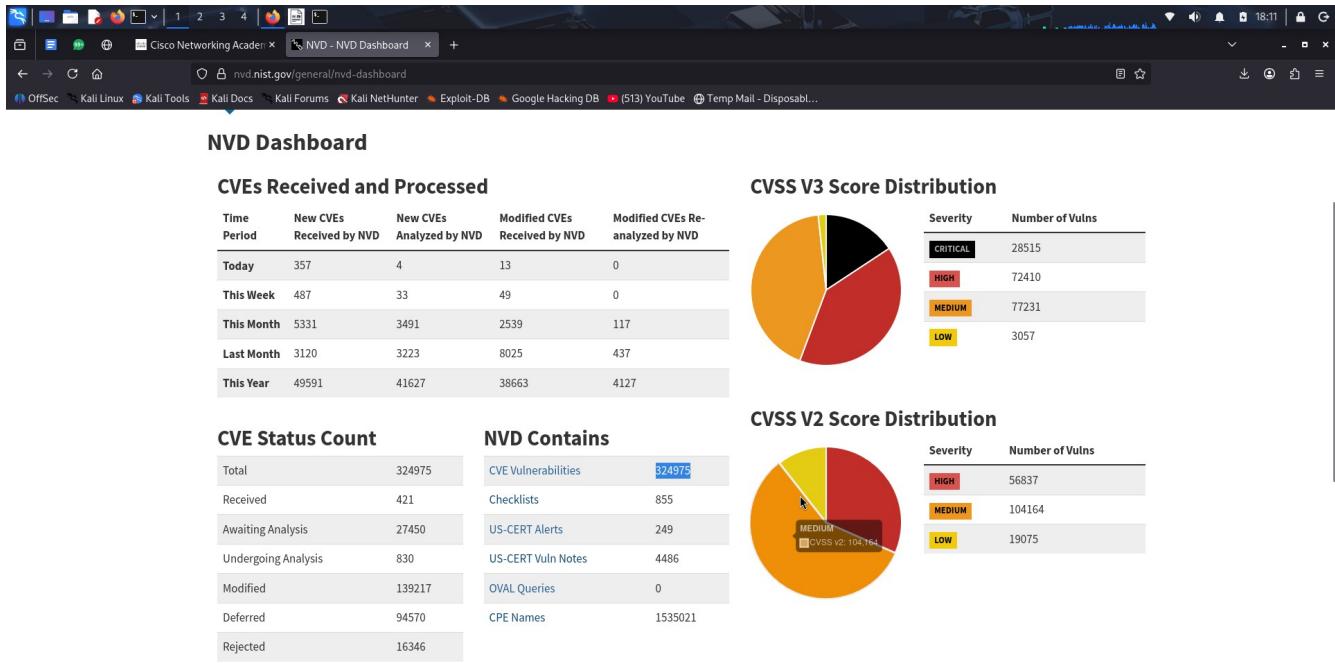
3. Click **General** to view and review General Information about the NVD. What is the relationship between the NVD and CVEs?

The screenshot shows the "General" page of the NVD. On the left is a sidebar with links for General, Vulnerabilities, Vulnerability Metrics, Products, Developers, Contact NVD, Other Sites, and Search. The main content area has three circular icons: "A Brief History of the NVD" (books), "CVEs and the NVD Process" (document with a path), and "CNAs and CVE Counting" (abacus). The "General Information" section contains a detailed description of the NVD's purpose and history, mentioning its creation in 1999, its evolution through iterations, and its role in vulnerability management. It also discusses the NVD's relationship with the CVE List and the work of the NIST Computer Security Division, Information Technology Laboratory.

Legal Disclaimer:

Here is where you can read the NVD legal disclaimer.

Expand the menu under **General** and click **NVD Dashboard**. How many CVE Vulnerabilities are contained in the NVD?



For information on how to cite the NVD, including the database's Digital Object Identifier (DOI), please consult NIST's Public Data Repository.

What is the most recent scored Vulnerability and what is the CVSS rating?

Last 20 Scored Vulnerability IDs & Summaries	CVSS Severity
CVE-2025-13806 - A security vulnerability has been detected in nutzam NutzBoot up to 2.6.0-SNAPSHOT. This impacts an unknown function of the file nutzboot-demo/nutzboot-demo-simple/nutzboot-demo-simple-web3j/src/main/java/io/nutz/demo/simple/module/EthModule.java ... read CVE-2025-13806	V3.1: 9.8 CRITICAL
Published: December 01, 2025; 12:16:00 AM -0500	
CVE-2025-12106 - Insufficient argument validation in OpenVPN 2.7_alpha1 through 2.7_rc1 allows an attacker to trigger a heap buffer over-read when parsing IP addresses	
Published: December 01, 2025; 8:16:00 AM -0500	
CVE-2025-55129 - HackerOne community member Kassem S.(kassem_s94) has reported that username handling in Revive Adserver was still vulnerable to impersonation attacks after the fix for CVE-2025-52672, via several alternate techniques. Homoglyphs based impersonatio... read CVE-2025-55129	
Published: December 01, 2025; 9:15:46 PM -0500	

Navigate back to the National Vulnerability Database page <https://nvd.nist.gov/>.

- Click **Vulnerability Metrics** in the menu on the left of the page.

What method is used to qualitatively measure the severity of vulnerabilities?

NVD - Vulnerability Metrics

An official website of the United States government. Here's how you know.

NIST

Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

NIST NATIONAL VULNERABILITY DATABASE NVD

- General** +
- Vulnerabilities** +
- Vulnerability Metrics** +
- Products** +
- Developers** +
- Contact NVD**
- Other Sites** +
- Search** +



Product Integration with NVD CVSS Calculators

[Common Vulnerability Scoring System](#)

Vulnerability Metrics

The Common Vulnerability Scoring System (CVSS) is a method used to supply a qualitative measure of severity. **CVSS is not a measure of risk.** CVSS v2.0 and CVSS v3.x consist of three metric groups: Base, Temporal, and Environmental. CVSS v4.0 is a bit different and consists of Base, Threat, Environmental and Supplemental metric groups. Metrics result in a numerical score ranging from 0 to 10. A CVSS assessment is also represented as a vector string, a compressed textual representation of the values used to derive the score. Thus, CVSS is well suited as a standard measurement system for industries, organizations, and governments that need accurate and consistent vulnerability severity scores. Two common uses of CVSS are calculating the severity of vulnerabilities discovered on one's systems and as a factor in prioritization of vulnerability remediation activities. The National Vulnerability Database (NVD) provides CVSS enrichment for all published CVE records.

The NVD supports Common Vulnerability Scoring System (CVSS) v2.0, v3.x and v4.0 standards. However, per the NVD CVSS v2.0 Retirement announcement, we no longer provide CVSS v2.0 assessments for newly published CVE records. The NVD provides CVSS assessments of Base metrics the innate characteristics of each vulnerability. The NVD does not currently provide assessments for Temporal or Threat metrics (metrics that change over time due to events external to the vulnerability), Environmental metrics (metrics customized to reflect the impact of the vulnerability to a particular organization) or Supplemental metrics (metrics used to provide additional context). However, the NVD does supply a CVSS calculator for each version of CVSS to allow users to assess non-Base metrics.

The CVSS specifications are owned and managed by FIRST.Org, Inc. (FIRST), a US-based non-profit organization, whose mission is to help computer security incident response teams across the world. The official CVSS documentation can be found at <https://www.first.org/cvss/>.

How many severity ratings does CVSS v3.0 have and what are they? **5: none,low,medium, high, critical**

NVD - Vulnerability Metrics

An official website of the United States government. Here's how you know.

Retirement announcement, we no longer provide CVSS v2.0 assessments for newly published CVE records. The NVD provides CVSS assessments of Base metrics the innate characteristics of each vulnerability. The NVD does not currently provide assessments for Temporal or Threat metrics (metrics that change over time due to events external to the vulnerability), Environmental metrics (metrics customized to reflect the impact of the vulnerability to a particular organization) or Supplemental metrics (metrics used to provide additional context). However, the NVD does supply a CVSS calculator for each version of CVSS to allow users to assess non-Base metrics.

The CVSS specifications are owned and managed by FIRST.Org, Inc. (FIRST), a US-based non-profit organization, whose mission is to help computer security incident response teams across the world. The official CVSS documentation can be found at <https://www.first.org/cvss/>.

NVD CVSS Calculators

[NVD CVSS v2.0 Calculator](#)

[NVD CVSS v3.x Calculator](#)

[NVD CVSS v4.0 Calculator](#)

Qualitative Severity Ratings

CVSS v2.0 Ratings		CVSS v3.x Ratings		CVSS v4.0 Ratings	
Severity	Severity Score Range	Severity	Severity Score Range	Severity	Severity Score Range
Low	0.0-3.9	None*	0.0	None*	0.0
Medium	4.0-6.9	Low	0.1-3.9	Low	0.1-3.9
High	7.0-10.0	Medium	4.0-6.9	Medium	4.0-6.9
		High	7.0-9.9	High	7.0-8.9
		Critical	9.0-10.0	Critical	9.0-10.0

The NVD notes qualitative severity ratings of "Low", "Medium", and "High" for CVSS v2.0 base score ranges in addition to the qualitative severity ratings for CVSS v3.x and CVSS v4.0 as they are defined in their respective specifications.

Note: The CVSS specification allows for the application of vector strings that result in a 0.0 severity score. However, NVD enrichment does not assess CVSS vector strings that have no impacts. Per the CVE Program's definition of a vulnerability, there should not be a CVE record counted that does not cause an impact to confidentiality, integrity, or availability.

NVD Specific CVSS Information

Incomplete Data

With some vulnerabilities, all of the information needed to assess CVSS vector strings may not be available. This typically happens when a

Part 4: Research Vulnerabilities in the Common Vulnerability Scoring System (CVSS)

Step 1: Explore CVSS.

- a. Launch the CVSS website and navigate to <https://first.org/cvss>
- b. Review the information on the CVSS.
- c. Investigate CVSS ratings by clicking **Specification Document** in the left menu.

What are the three metrics that compose a CVSS rating?

The screenshot shows a web browser window with the URL www.first.org/cvss/v4-0/specification-document. The page title is "Common Vulnerability Scoring System version 4.0: Specification Document". The content includes an introduction, details about metric groups, and a table of contents for the document. The sidebar on the left lists various CVSS resources like a calculator, specification document, user guide, examples, and frequently asked questions. The right sidebar contains a table of contents for the specification document, which includes sections for introduction, metrics, base metrics, threat metrics, environmental metrics, supplemental metrics, qualitative severity rating scale, vector string, and version history.

How many metrics compose the Base Metric group of a CVSS? What are they? **8**

1.1. Metrics

CVSS is composed of four metric groups: Base, Threat, Environmental, and Supplemental, each consisting of a set of metrics, as shown in Figure 1.

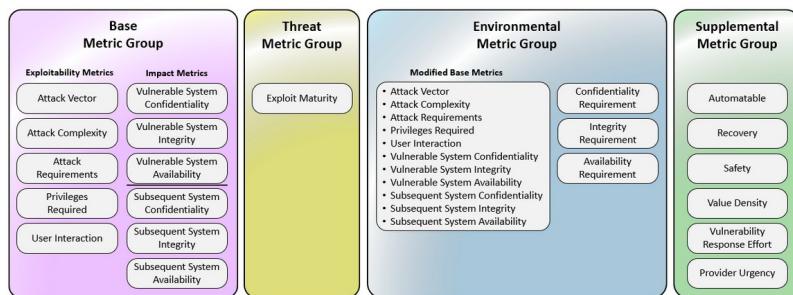


Figure 1: CVSS Metric Groups

The Base metric group represents the intrinsic characteristics of a vulnerability that are constant over time and across user environments. It is composed of two sets of metrics: the Exploitability metrics and the Impact metrics.

The Exploitability metrics reflect the ease and technical means by which the vulnerability can be exploited. That is, they represent characteristics of the “thing that is vulnerable”, which we refer to formally as the “vulnerable system”. The Impact metrics reflect the direct consequence of a successful exploit, and represent the consequence to the “things that suffer the impact”, which may include Impact on the vulnerable system and/or the downstream impact on what is formally called the “subsequent system(s)”.

While the vulnerable system is typically a software application, operating system, module, driver, etc. (or possibly a hardware device), the subsequent system could be any of those examples but also includes human safety. This potential for measuring the impact of a vulnerability other than the vulnerable system, was a key feature introduced with CVSS v3.0. This property (formerly known as “scope”), is captured by the separation of impacts to the vulnerable system and to subsequent systems, discussed later.

The Threat metric group reflects the characteristics of a vulnerability related to threat that may change over time but not necessarily across user environments. For example, confirmation that the vulnerability has neither been exploited nor has any proof-of-concept exploit code or instructions publicly available will lower the resulting CVSS score. The values found in this metric group may change over time.

[Help](#)

1. Click Examples in the left menu.

2. Click the link for CVSS version 3.1 examples.

Common Vulnerability Scoring System v3.1: Examples

Also available in PDF format (533KB) [Download](#).

1. Resources & Links

Below are useful references to additional CVSS v3.1 documents.

Resource	Location
Specification Document	Includes metric descriptions, formulas, and vector string. Available at https://www.first.org/cvss/specification-document .
User guide	Includes further discussion of CVSS v3.1, a scoring rubric, and a glossary. Available at https://www.first.org/cvss/user-guide .
Examples document	Includes examples of CVSS v3.1 scoring in practice. Available at https://www.first.org/cvss/examples .
CVSS v3.1 calculator	Reference implementation of the CVSS v3.1 equations available at https://www.first.org/cvss/calculator/3.1 .
XML schema	Schema definition available at http://www.first.org/cvss/cvss-v3.1.xsd .
CVSS v3.1 main page	Main page for all other CVSS resources: https://www.first.org/cvss .

2. Introduction

This document demonstrates how to apply the CVSS version 3.1 standard to score specific vulnerabilities. A summary of each vulnerability is provided, along with the attack being scored. CVSS version 2.0 scores are provided to show scoring differences between the two standards. Cases where the CVSS version 3.1 metric values differ from their CVSS version 3.0 counterparts are also discussed.

Details of the vulnerabilities and attacks were sourced primarily from the National Vulnerability Database (NVD) at <https://nvd.nist.gov/vuln>. Information from additional sources was also used when more details were required.

Important Note: The scoring models assume target systems are employing the vulnerable configuration if applicable.

Table of Contents

- Common Vulnerability Scoring System v3.1: Examples
- 1. Resources & Links
- 2. Introduction
- 3. MySQL Stored SQL Injection (CVE-2013-0375)
 - Vulnerability
 - Attack
 - CVSS v2.0 Base Score: 5.5
 - CVSS v3.1 Base Score: 6.4
- 4. SSL3 POODLE Vulnerability (CVE-2014-3566)
 - Vulnerability
 - Attack
 - CVSS v2.0 Base Score: 4.3
 - CVSS v3.1 Base Score: 3.1
- 5. VMware Guest to Host Escape Vulnerability (CVE-2012-1516)
 - Vulnerability
 - Attack
 - CVSS v2.0 Base Score: 9.0
 - CVSS v3.1 Base Score: 9.9
- 6. Apache Tomcat XML Parser Vulnerability (CVE-2009-0783)
 - Vulnerability
 - Attack
 - CVSS v2.0 Base Score: 4.6
 - CVSS v3.1 Base Score: 4.2
- 7. Cisco IOS Arbitrary Command Execution Vulnerability (CVE-2012-0384)
 - Vulnerability
 - Attack
 - CVSS v2.0 Base Score: 8.5
 - CVSS v3.1 Base Score: 7.2
- 8. Apple iWork Denial of Service Vulnerability (CVE-2015-1098)
 - Vulnerability

3. Scroll down the page and review the example CVEs and how their CVSS v3.1 Base Scores were calculated.
4. Observe the Values given for each metric that makes up the CVSS score.

CVSS v3.1 Examples

CVSS v3.1 Base Score: 6.4

Metric	Value	Comments
Attack Vector	Network	The attacker connects to the exploitable MySQL database over a network.
Attack Complexity	Low	Replication must be enabled on the target database. Following the guidance in Section 2.1.2 of the Specification Document that was added in CVSS v3.1, we assume the system is configured in this way.
Privileges Required	Low	The attacker requires an account with the ability to change user-supplied identifiers, such as table names. Basic users do not get this privilege by default, but it is not considered a sufficiently trusted privilege to warrant this metric being High.
User Interaction	None	No user interaction is required as replication happens automatically.
Scope	Changed	The vulnerable component is the MySQL server database that the attacker logs into to perform the attack. The impacted component is a remote MySQL server database (or databases) that this database replicates to.
Confidentiality	Low	The injected SQL runs with high privilege and can access information the attacker should not have access to. Although this runs on a remote database (or databases), it may be possible to exfiltrate the information as part of the SQL statement. The malicious SQL is injected into SQL statements that are part of the replication functionality, preventing the attacker from executing arbitrary SQL statements.
Integrity	Low	The injected SQL runs with high privilege and can modify information the attacker should not have access to. The malicious SQL is injected into SQL statements that are part of the replication functionality, preventing the attacker from executing arbitrary SQL statements.
Availability	None	Although injected code is run with high privilege, the nature of this attack prevents arbitrary SQL statements being run that could affect the availability of MySQL databases.

4. SSLv3 POODLE Vulnerability (CVE-2014-3566)

Vulnerability

The SSL protocol 3.0, as used in OpenSSL through 1.0.1 and other products, uses nondeterministic CBC padding, which makes it easier for man in the middle attackers to obtain plaintext data via a padding-oracle attack, aka the "POODLE" (Padding Oracle on Downgraded Legacy Encryption) issue.

15. Juniper Proxy ARP Denial of Service Vulnerability (CVE-2013-6014)
16. Cantemo Portal Stored Cross-site Scripting Vulnerability (CVE-2019-7551)
17. Adobe Acrobat Buffer Overflow Vulnerability (CVE-2009-0658)
18. Microsoft Windows Bluetooth Remote Code Execution Vulnerability (CVE-2011-1265)
19. Apple iOS Security Control Bypass Vulnerability (CVE-2014-2019)
20. SearchBlox Cross-Site Request Forgery Vulnerability (CVE-2015-0970)
21. SSL/TLS MITM Vulnerability (CVE-2014-0224)

Research the CVSS ratings of the CWEs recorded in Part 1, Step 2.

1. Navigate to www.cve.org.
2. In the search box enter **CVE-2021-41617** and click **Search**.

CVE Record: CVE-2021-41617

CVE-2021-41617

Required CVE Record Information

CNA: MITRE Corporation

Published: 2021-09-26 Updated: 2023-12-26

Description

sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process; if the configuration specifies running the command as a different user.

Product Status

Learn more

Information not provided

References 14 Total

- <https://www.openssh.com/security.html>
- <https://www.openwall.com/lists/oss-security/2021/09/26/1>
- <https://www.openssh.com/txt/release-8.8>

On This Page

Required CVE Record Information

CNA: MITRE Corporation
CVE Program

3. On a new tab type:**CVE-2021-41617** to view additional information on the NVD. Open the National Vulnerability Database to view details about the CVE.
4. Scroll to the **Severity** section and ensure that **CVSS Version 3.x** is selected.

Observe the values for the eight CVSS Base metrics in the **Vector**. The corresponding numerical score of these values combine to give a base score of 7.0 HIGH.

CVSS Version 3.x

Base Score: 7.0 HIGH

Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

URL	Source(s)	Tag(s)
https://bugzilla.suse.com/show_bug.cgi?id=1190975	CVE, MITRE	Issue Tracking, Patch, Third Party Advisory
https://lists.debian.org/debian-its-announce/2023/12/msg00017.html	CVE, MITRE	
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/6XJIONMHMKZDTMHBQR5TNLF2WDGWE/	CVE, MITRE	
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/6XJIONMHMKZDTMHBQR5TNLF2WDGWE/	CVE, MITRE	

5. In a separate browser window, navigate to the CVSS 3.1 Calculator at <https://www.first.org/cvss/calculator/3.1>.
6. In the Base Score calculator, click the metric names that correspond to the Vector on the NVD page. (**Vector:** CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H). What Base Score is calculated by the CVSS Calculator? **7.0**

The screenshot shows the Common Vulnerability Scoring System (CVSS) Version 3.1 Calculator on the FIRST website. The calculator interface includes sections for Attack Vector (AV), Attack Complexity (AC), Privileges Required (PR), User Interaction (UI), Scope (S), Confidentiality (C), Integrity (I), and Availability (A). The final output is a Vector String: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H and a Temporal Score of 7.0.

What is the relationship between CVE, CWE, NVD, and CVSS? **CVE lists vulnerabilities that have been discovered, CWE classifies these vulnerabilities, NVD provides details, and CVSS provides severity ratings.**