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

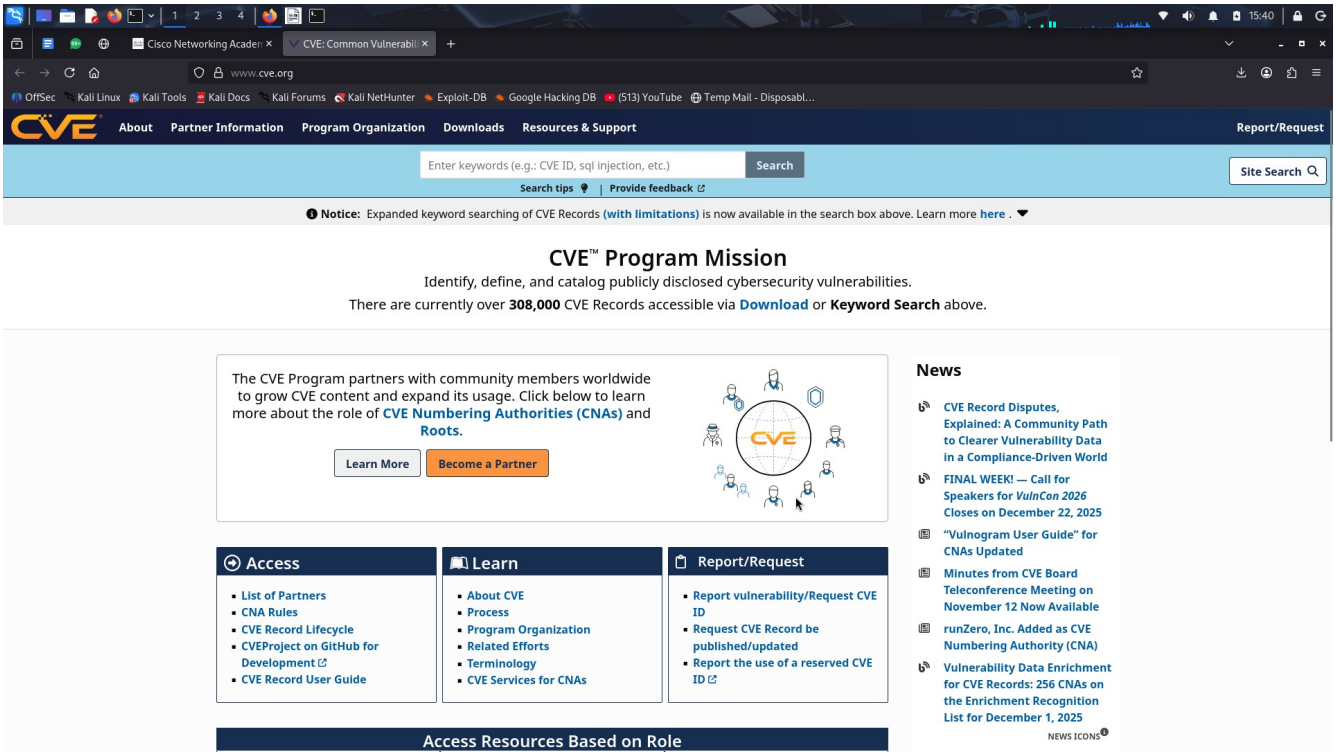
- Computer with internet connection

Instructions

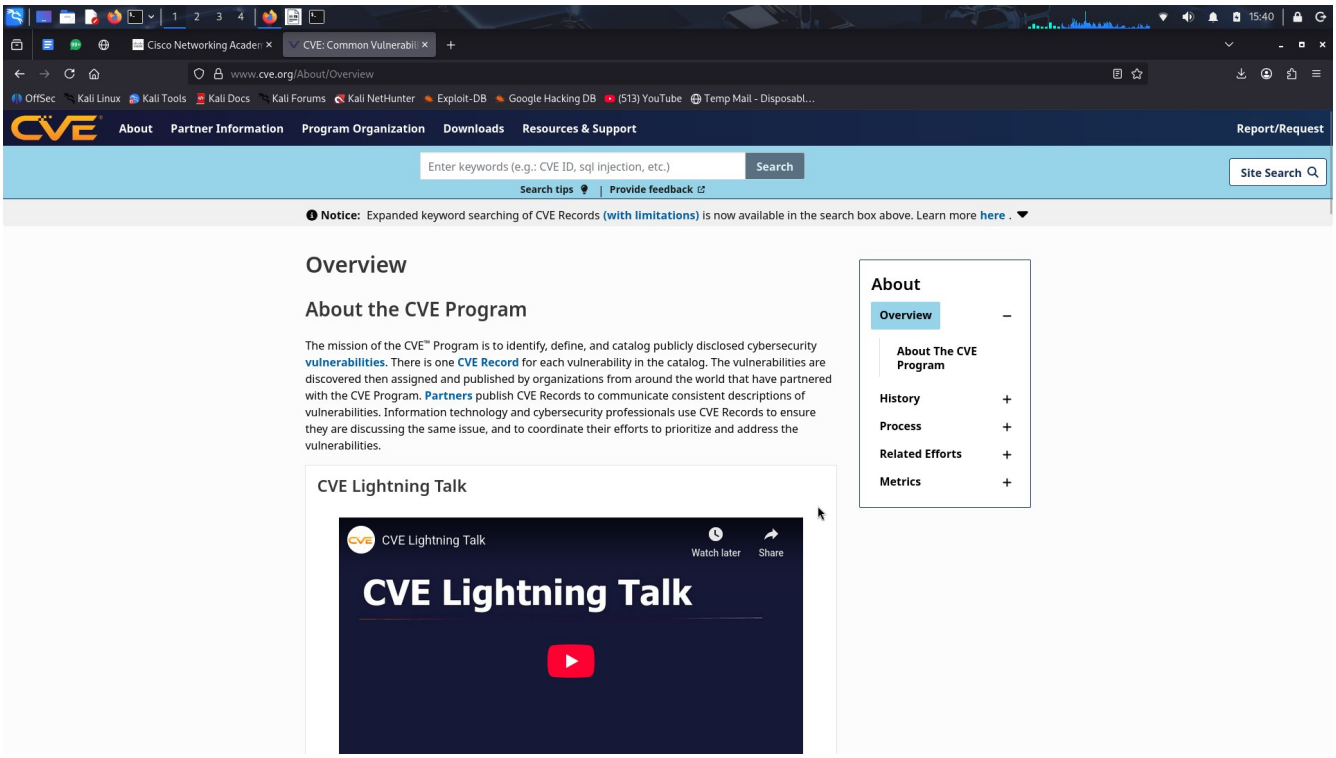
Part 1: Investigate Common Vulnerabilities and Exposures (CVEs)

Step 1: Explore CVE.

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



1. Select **About > Overview** in the menu.



2. View the CVE Program Overview video.
3. 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

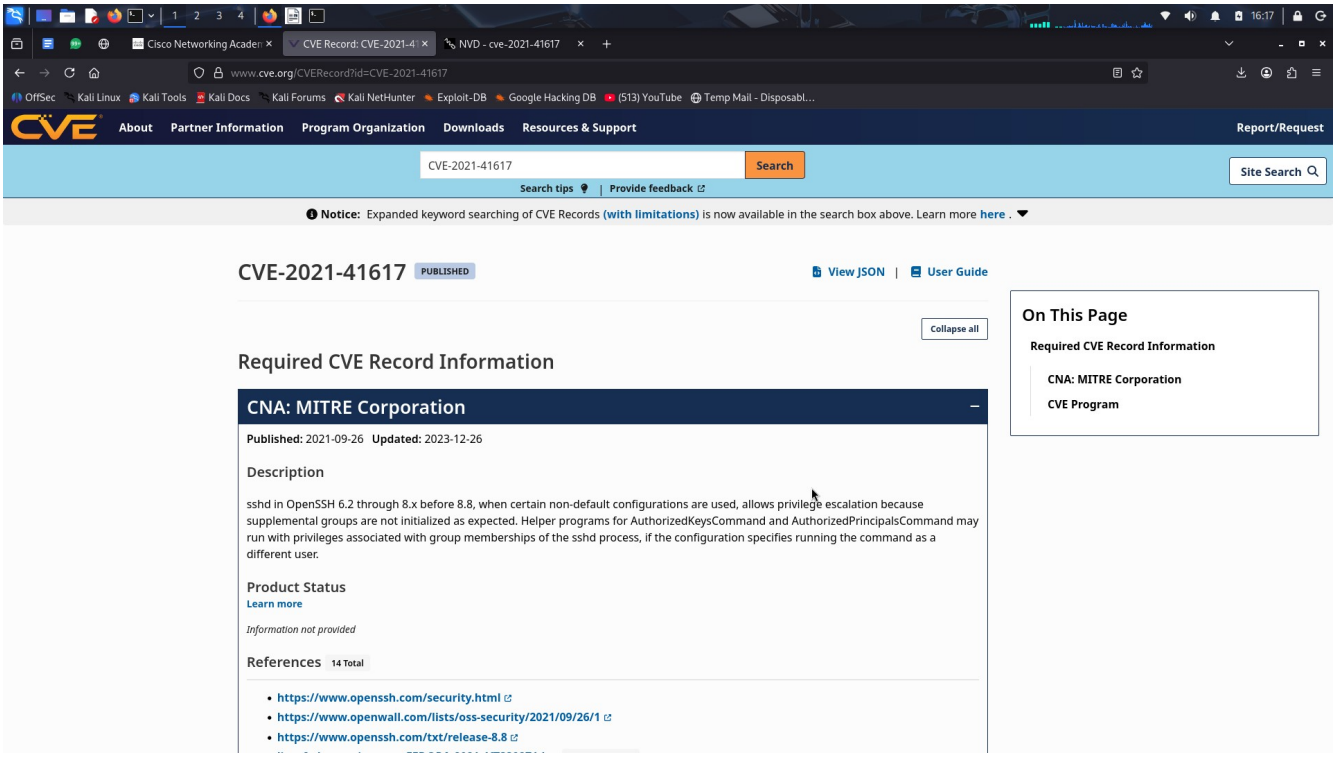
Show Answer

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**.



What versions of OpenSSH are subject to this vulnerability?

Answer Area

OpenSSH 6.2 through 8.x before 8.8

Show Answer

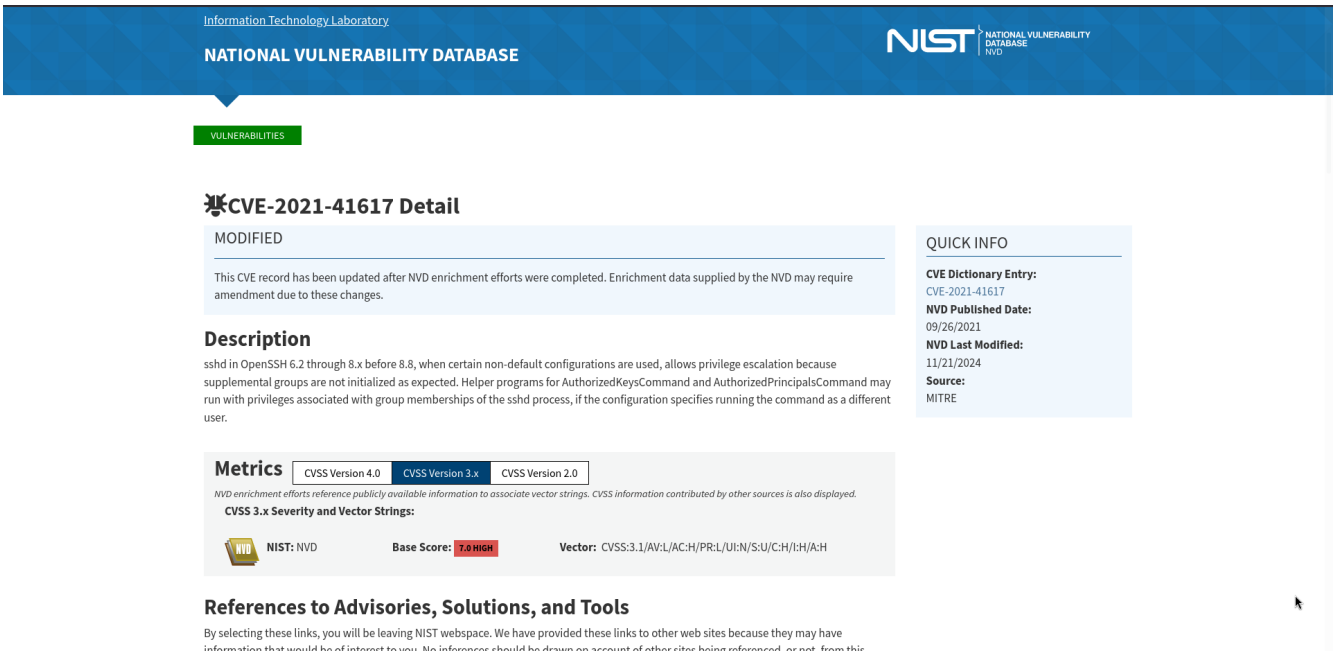
When was this CVE last updated?

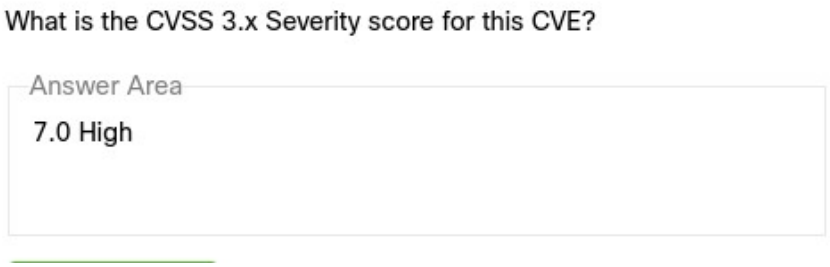
Answer Area

2023-12-26

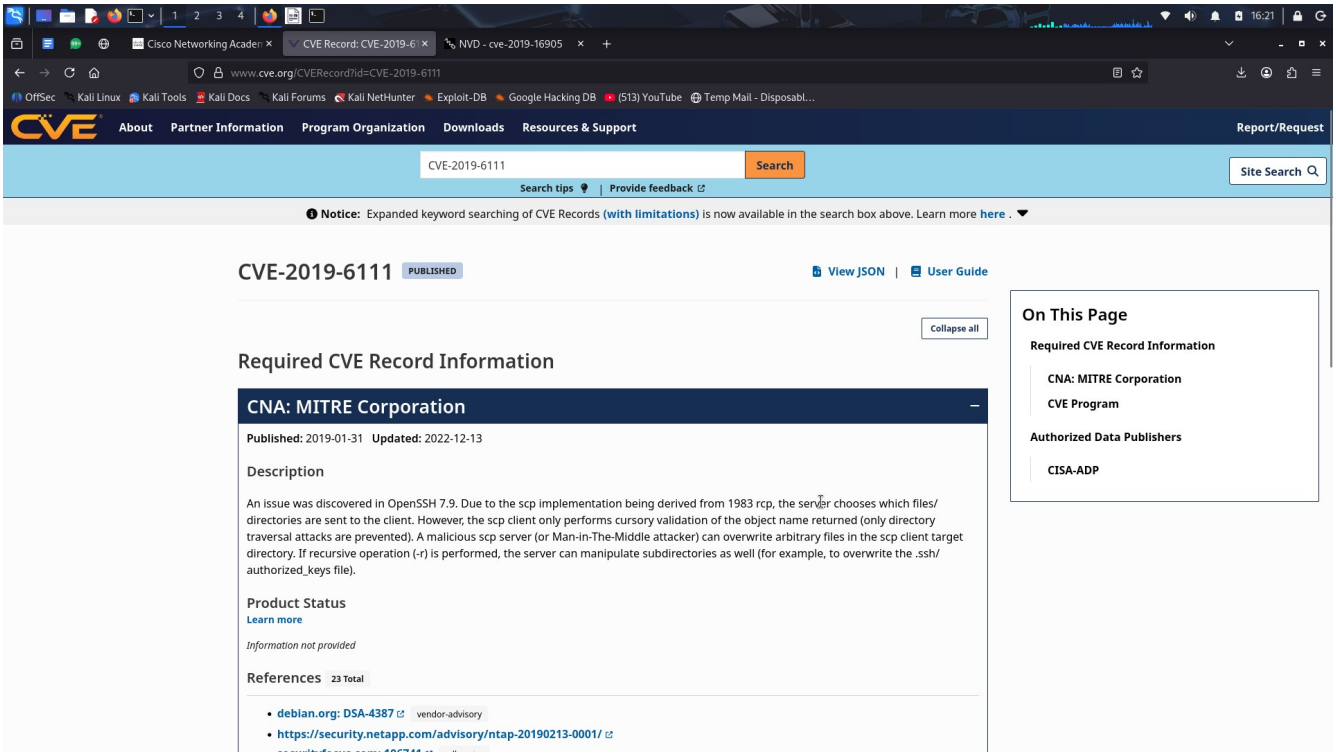
Show Answer

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





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



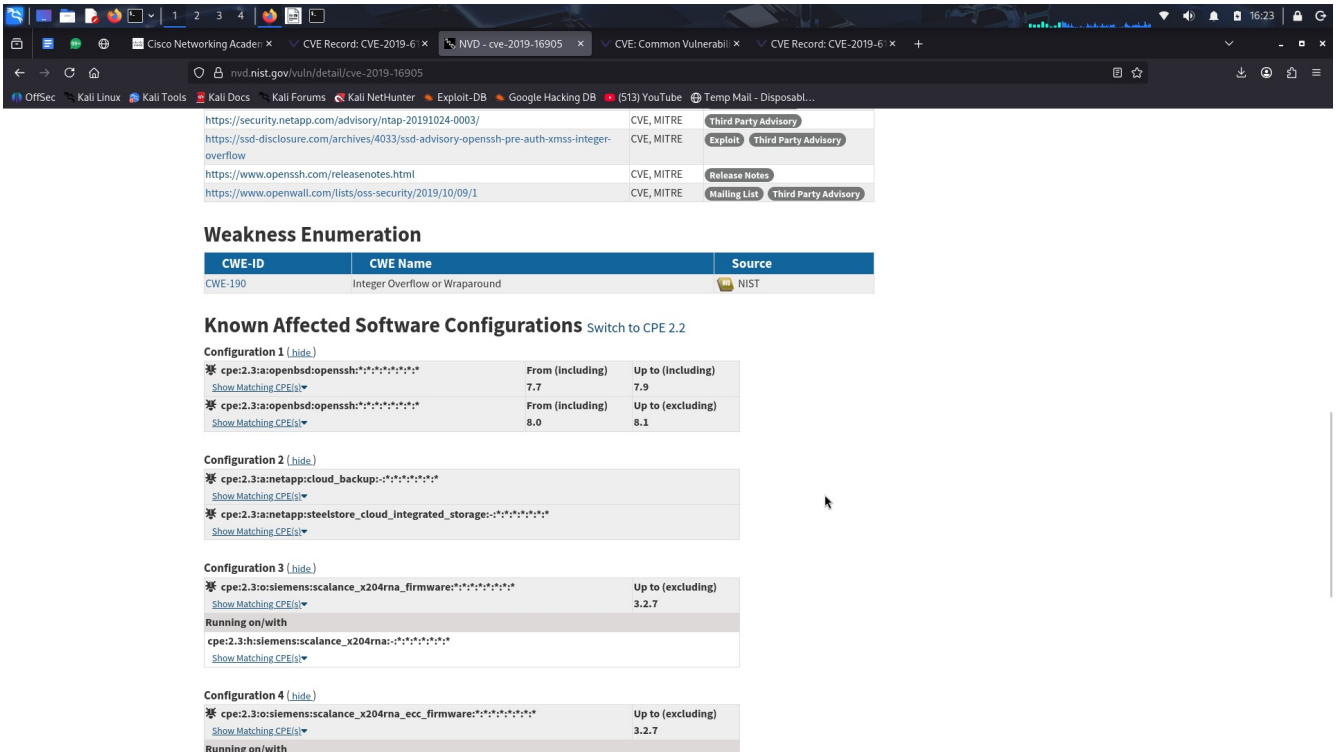
Which of these CVEs involves Man-in-the-Middle attacks from a malicious SCP server?

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.



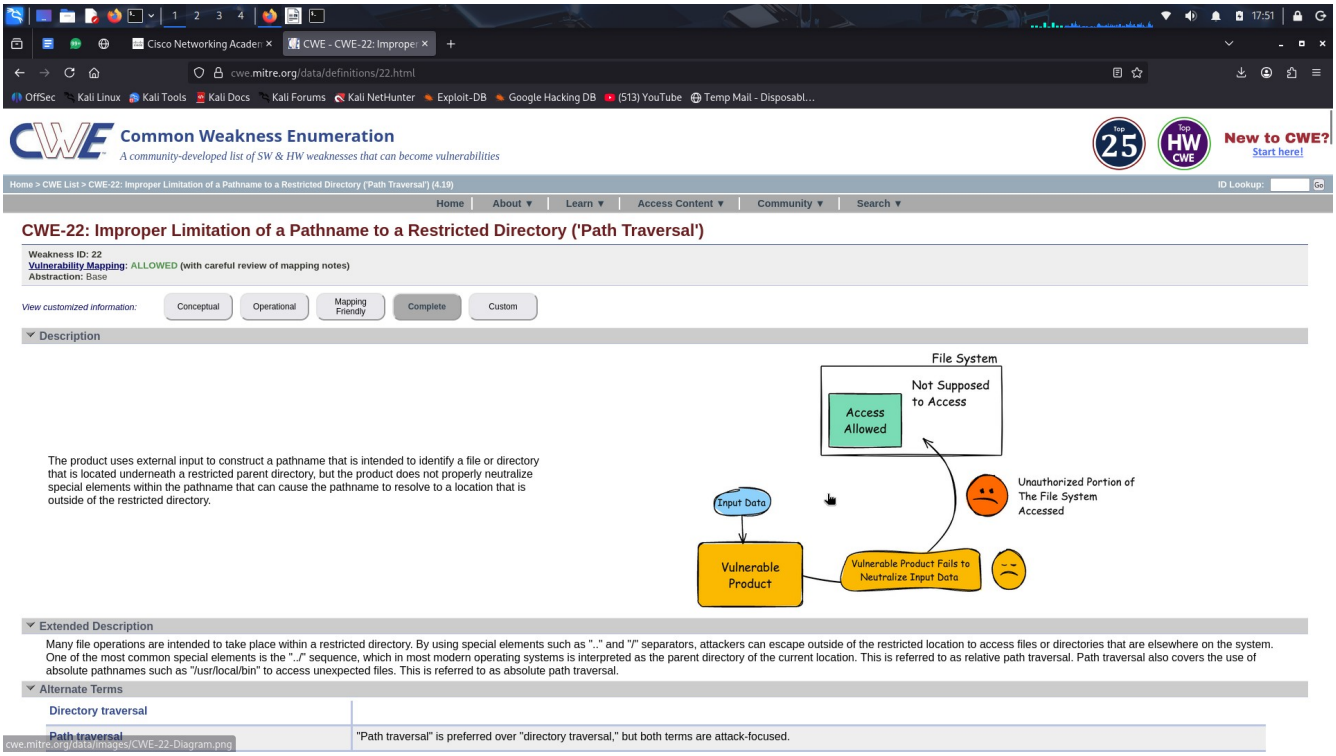
Part 2: Explore Common Weakness Enumeration (CWE)

Step 1: Explore CWE.

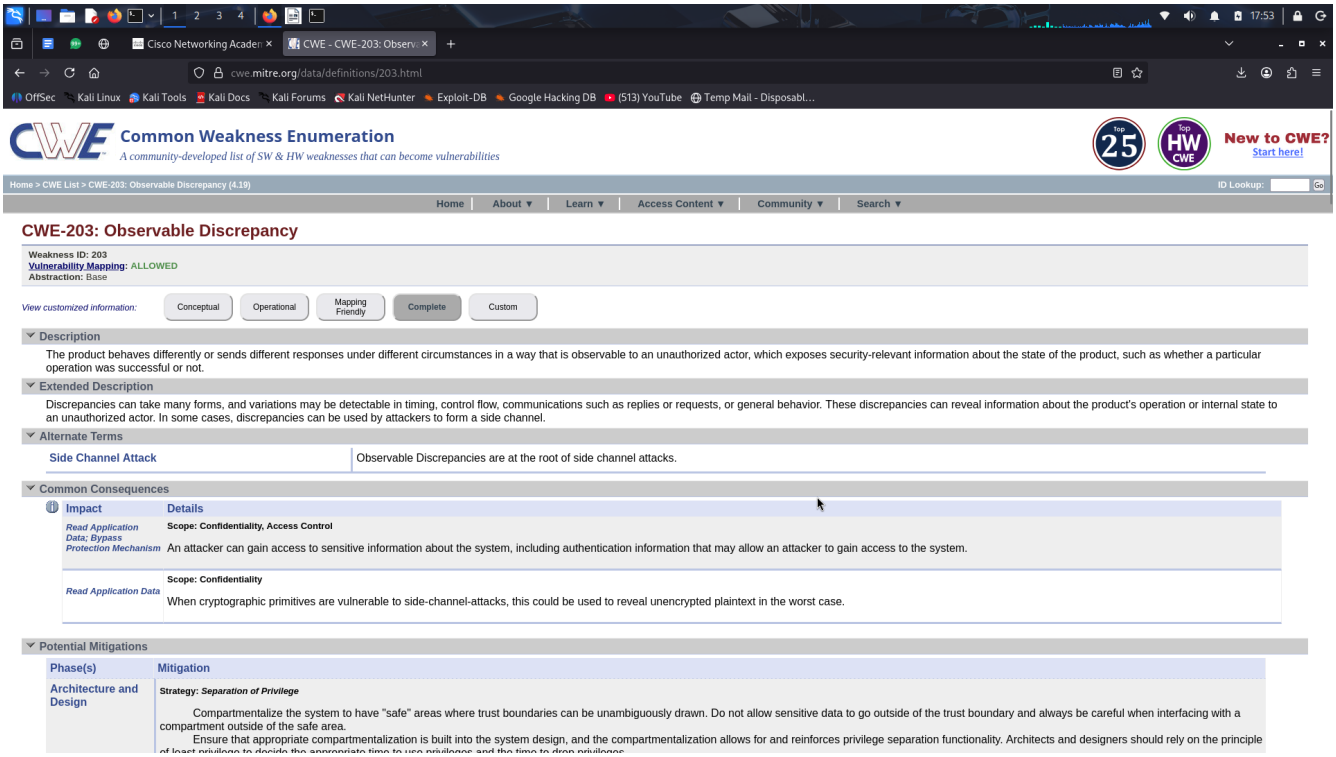
a. Launch the CWE website and navigate to https://cwe.mitre.org.
b. Explore the CVE program.by selecting **About** > **Overview** in the menu.

What is the goal of CWE? T**o 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.

1. 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?



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

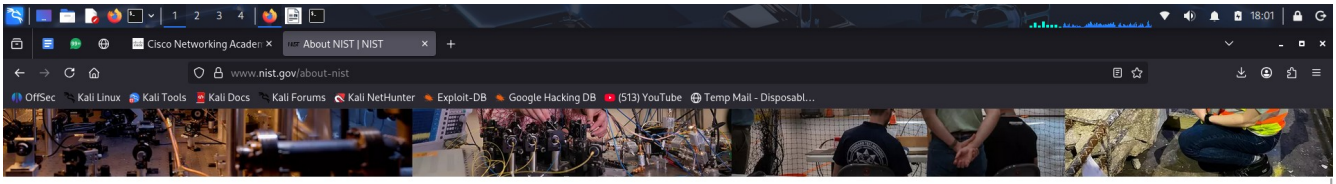


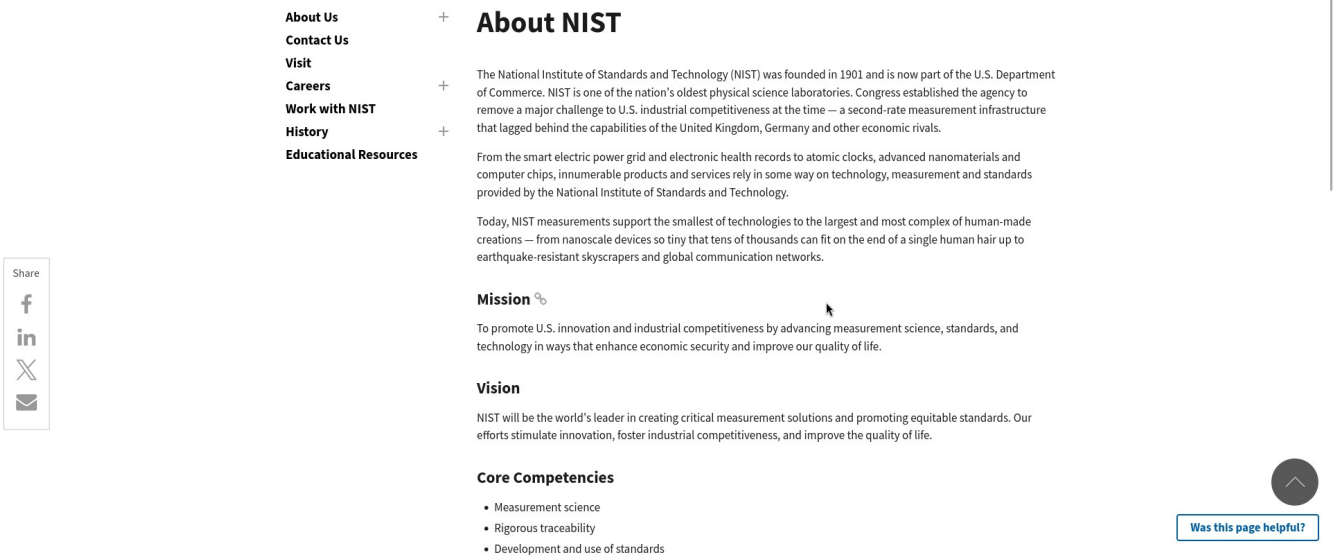
Part 3: Investigate National Institute of Standards and Technology (NIST) Vulnerability Resources

Step 1: Explore NIST.

a. Launch the NIST website by navigating to https://www.nist.gov.

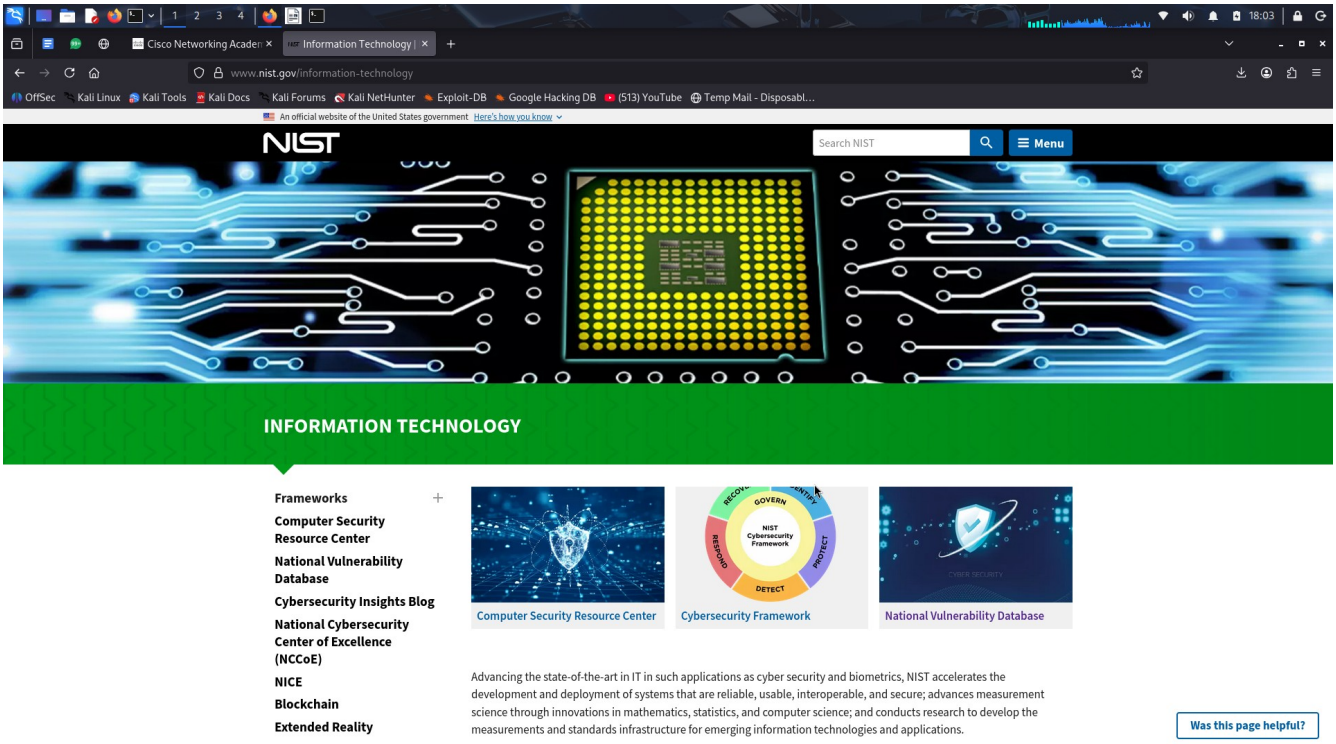
b. Select **About NIST** > **About Us** in the menu and review the overview of NIST.



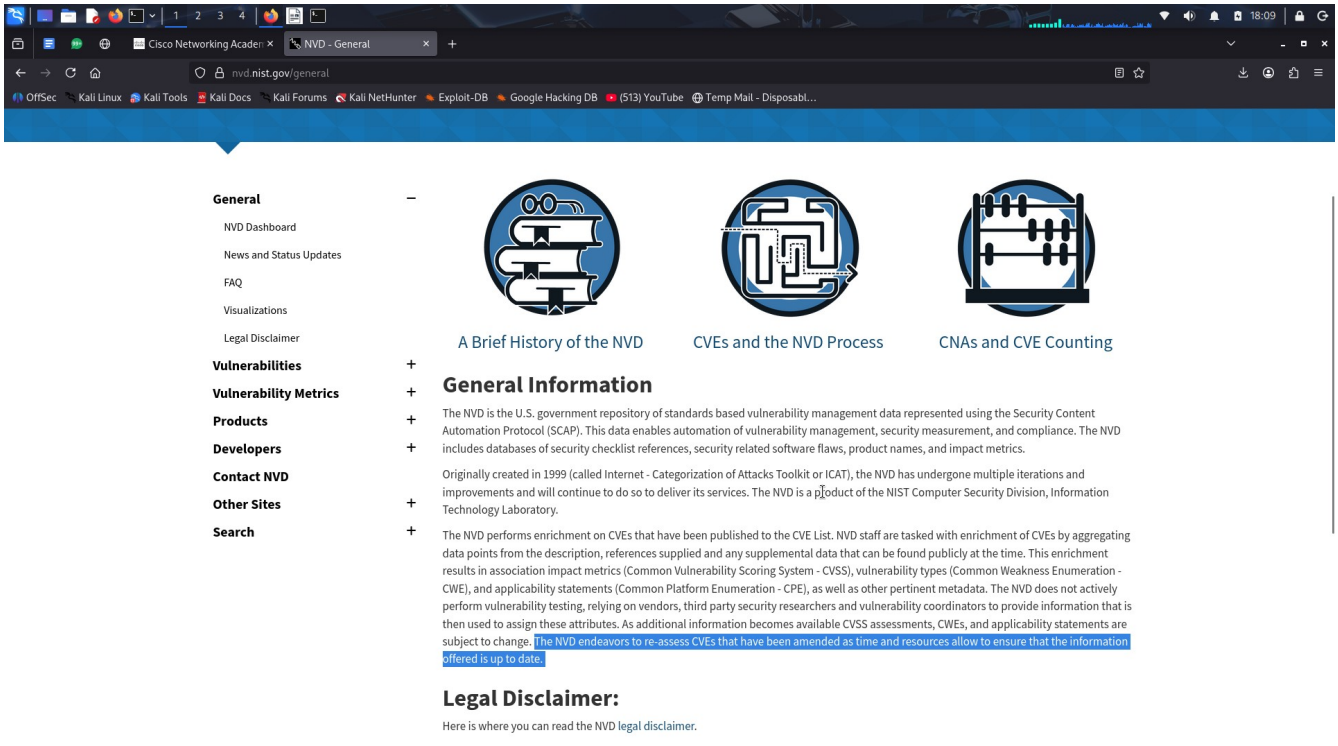


Explore the National Vulnerability Database (NVD).

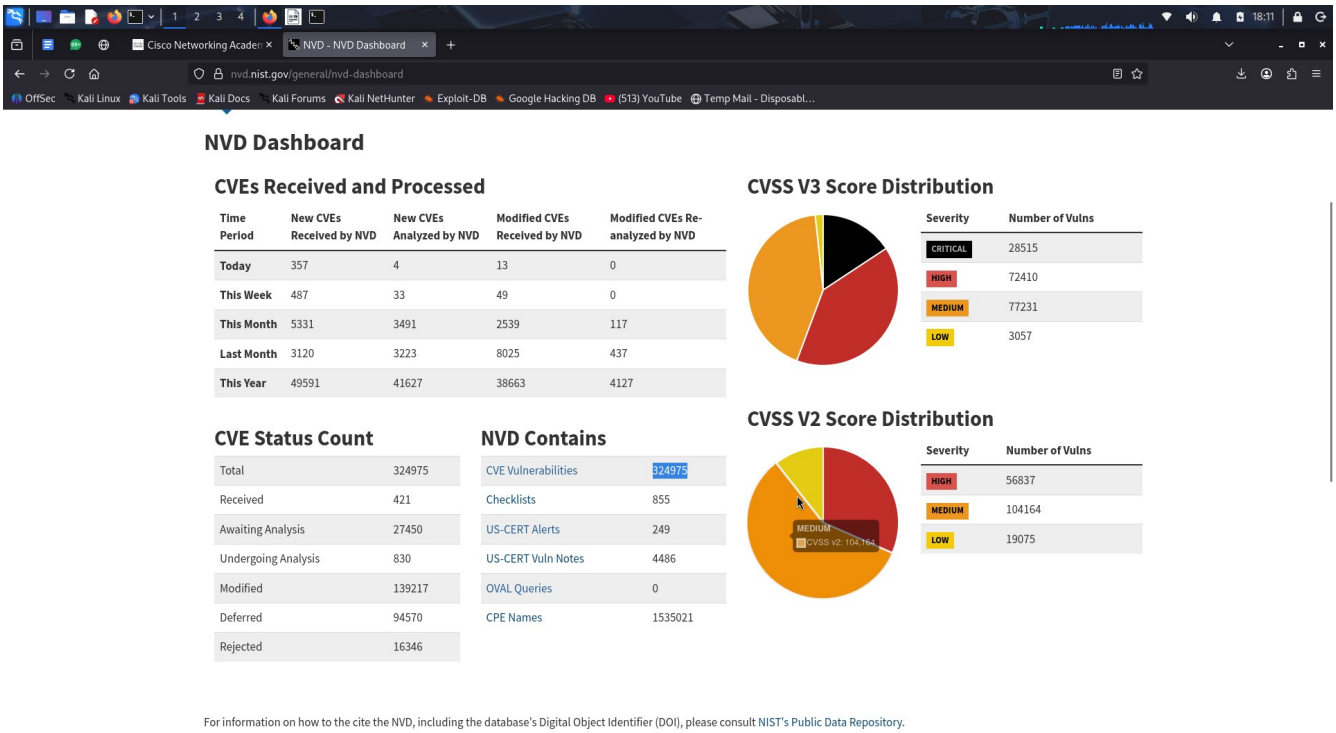
1. Return to the NIST home page and select **What We Do** > **Information Technology** in the menu.
2. Select **National Vulnerability Database** in the **Featured Content** list.



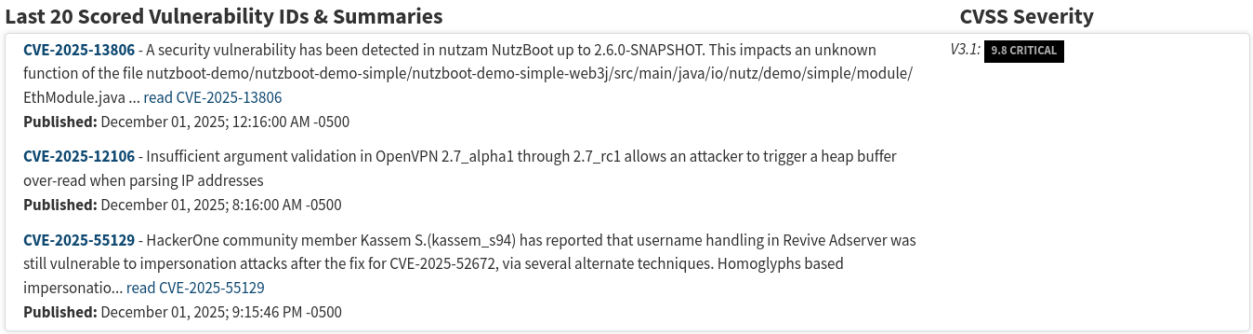
3. Click **General** to view and review General Information about the NVD. What is the relationship between the NVD and CVEs?



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



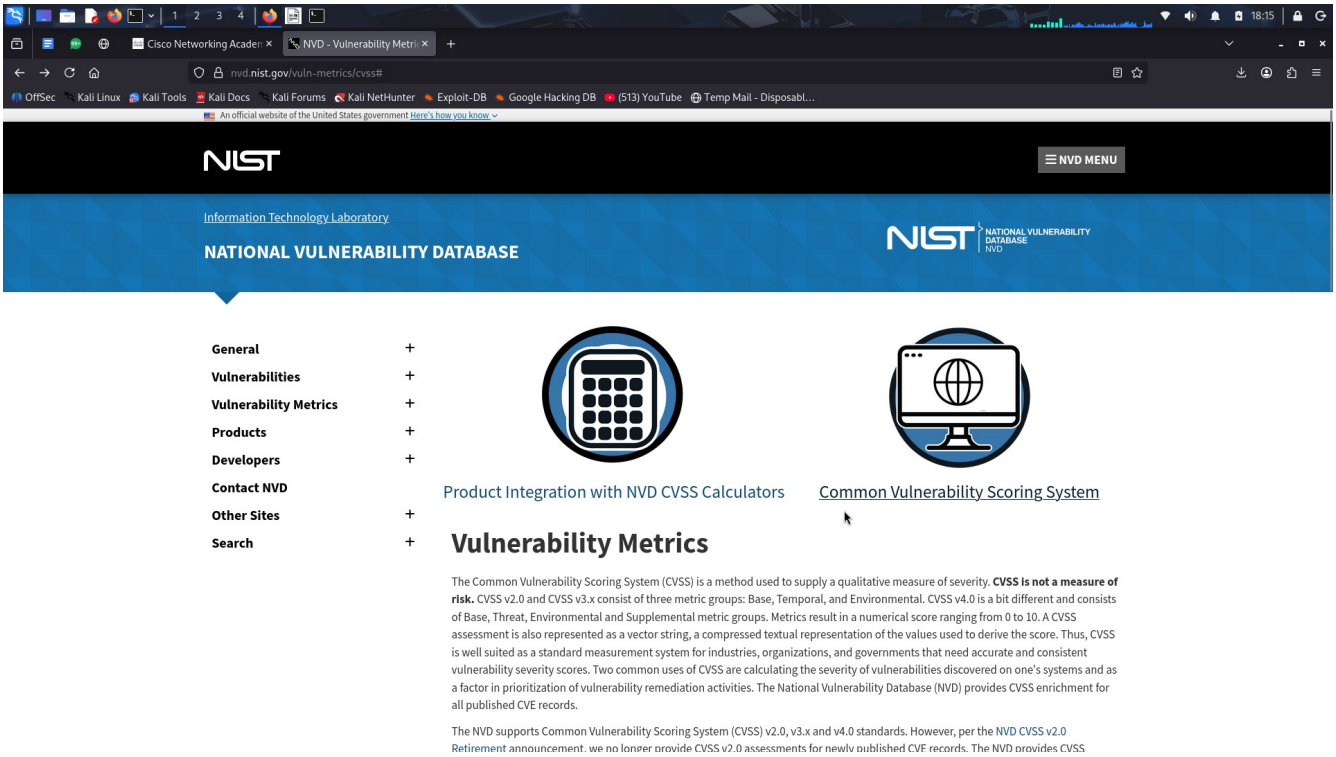
What is the most recent scored Vulnerability and what is the CVSS rating?



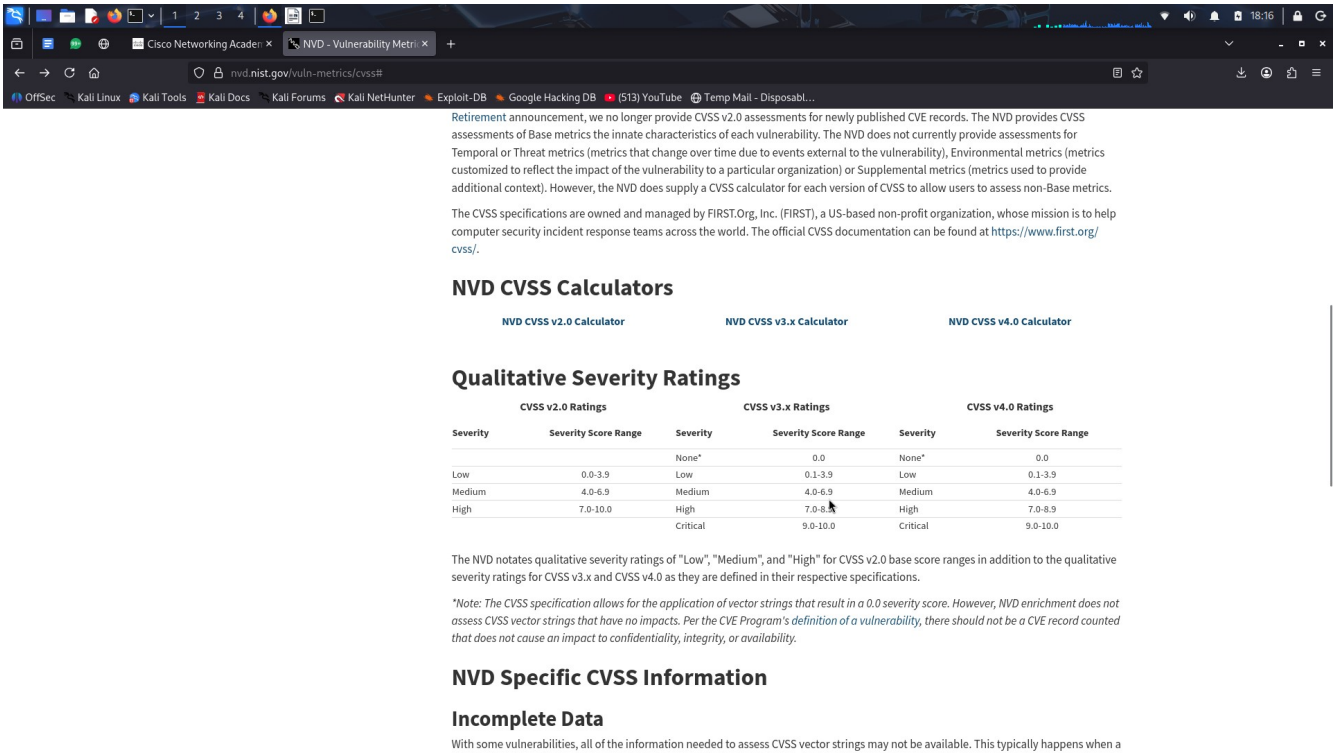
Navigate back to the National Vulnerability Database page https://nvd.nist.gov/.

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

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



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

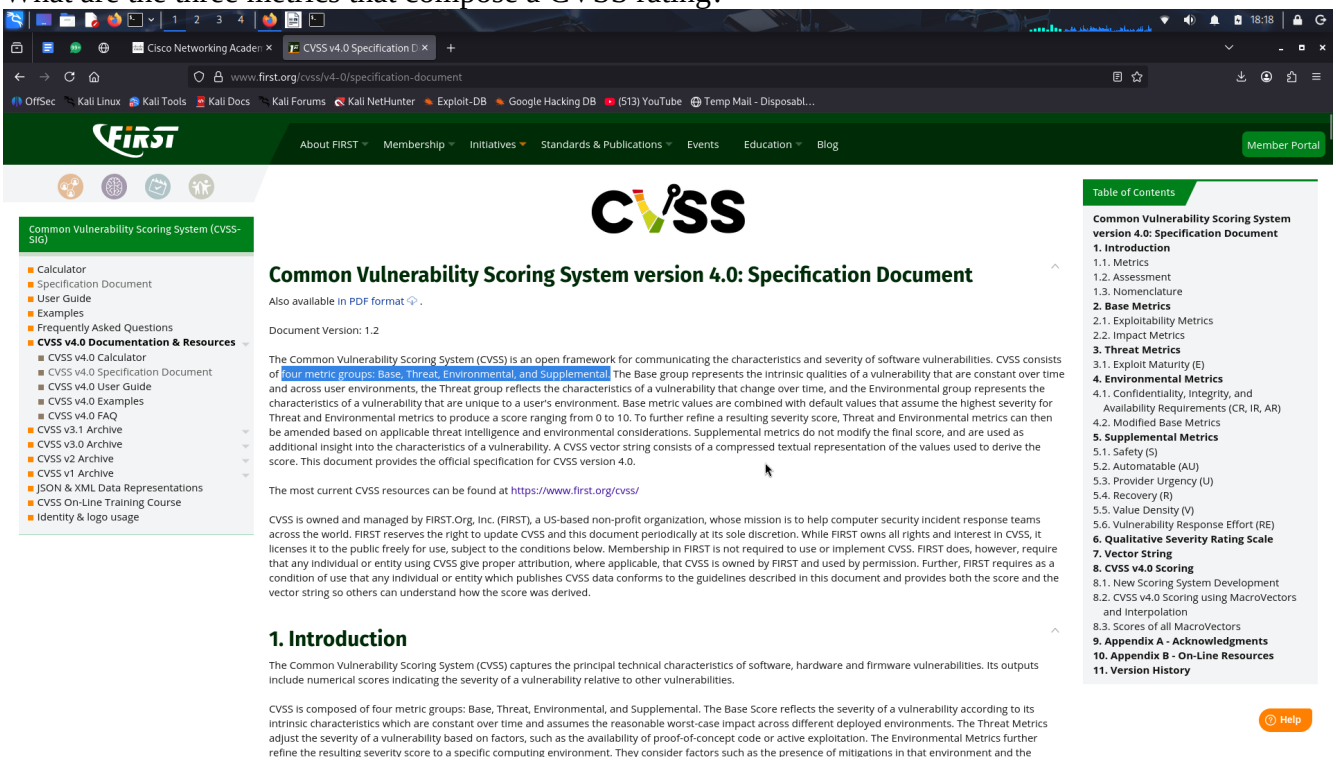


Part 4: Research Vulnerabilities in the Common Vulnerability Scoring System (CVSS)

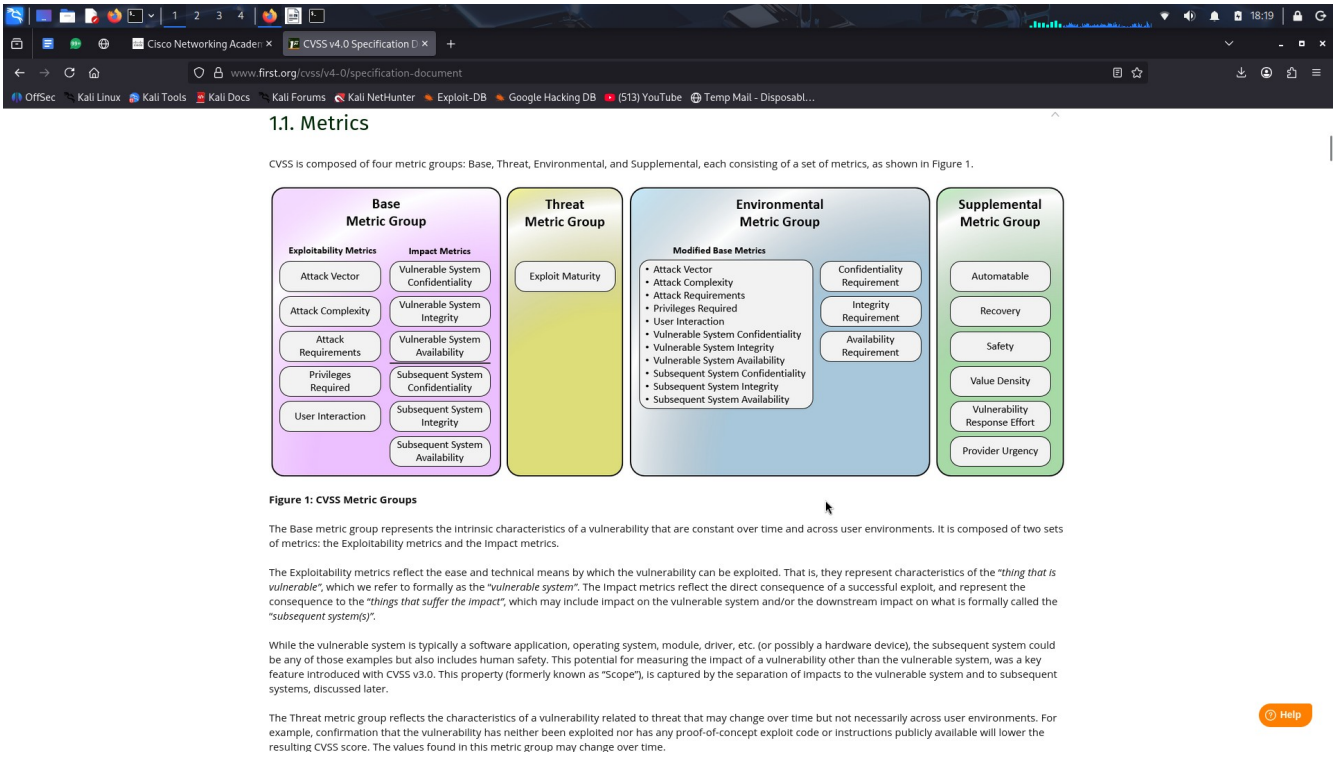
Step 1: Explore CVSS.

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.

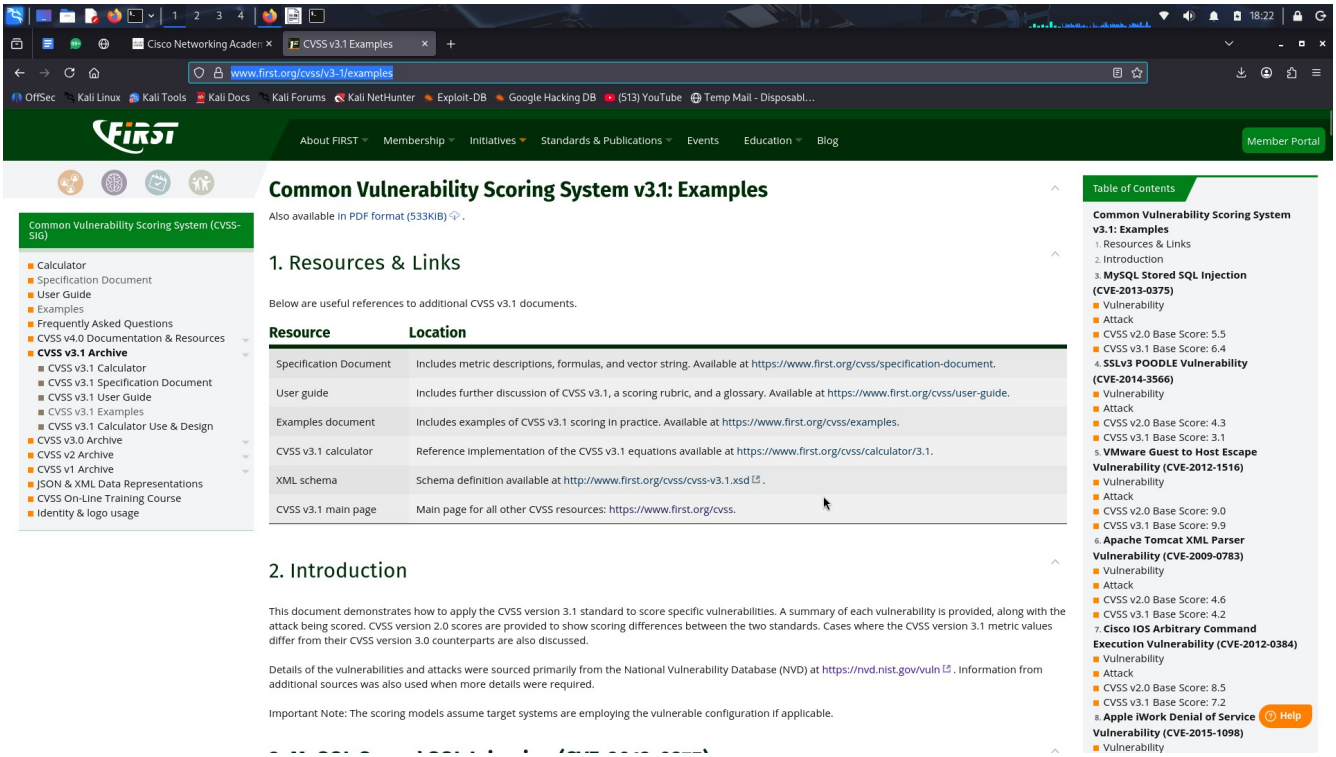
What are the three metrics that compose a CVSS rating?



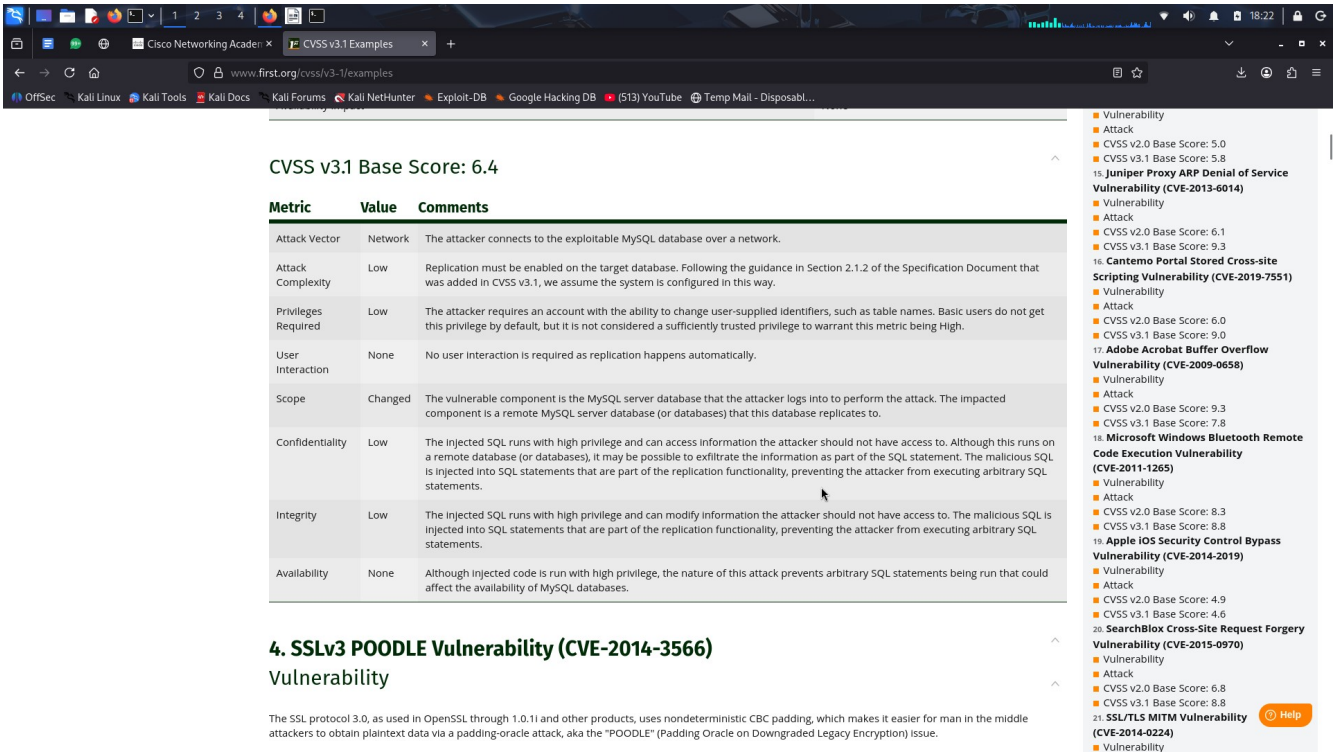
How many metrics compose the Base Metric group of a CVSS? What are they? **8**



1. Click **Examples** in the left menu.
2. Click the link for **CVSS version 3.1** examples.

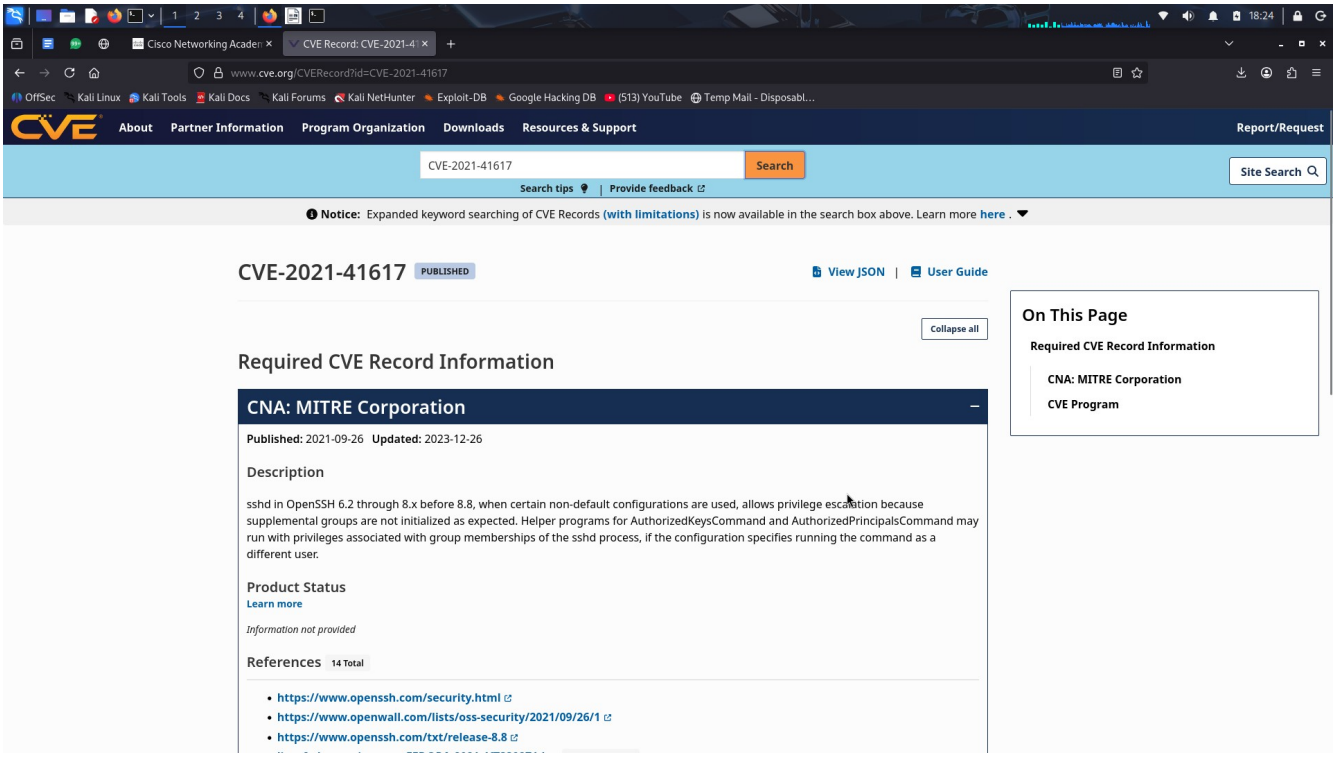


3. Scroll down the page and review the example CVEs and how their CVSS v3.1 Base Scores were calculated.
4. Observe the Values given for each metric that makes up the CVSS score.



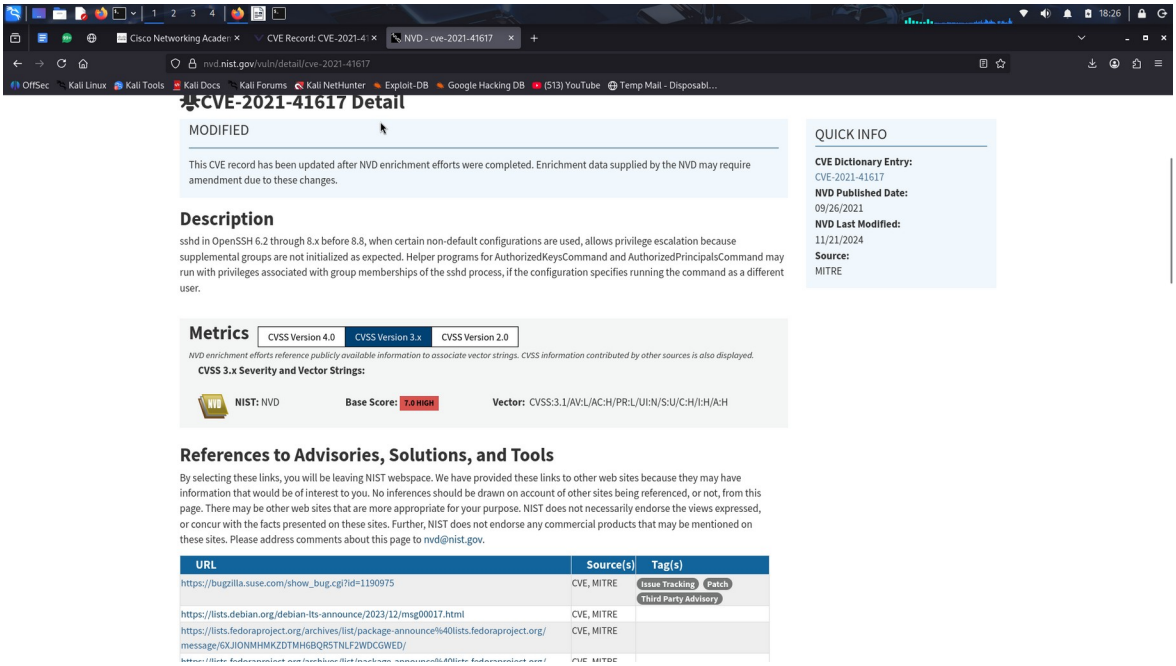
Research the CVSS ratings of the CWEs recorded in Part 1, Step 2.

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

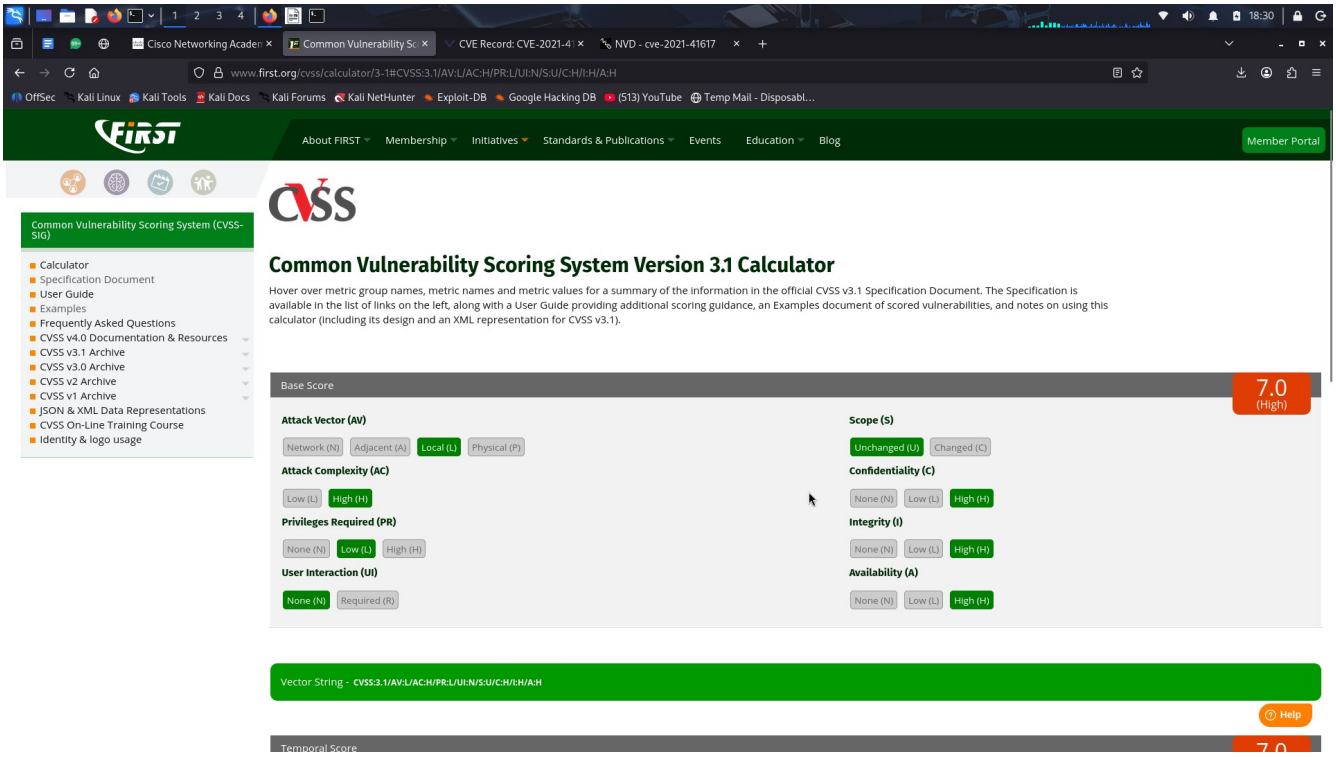


3. On a new tab type**:CVE-2021-41617** to view additional information on the NVD. Open the National Vulnerability Database to view details about the CVE.
4. Scroll to the **Severity** section and ensure that **CVSS Version 3.x** is selected.

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.



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**



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.**