

Module 05: Vulnerability Analysis

Lab 1: Perform Vulnerability Research with Vulnerability Scoring Systems and Databases

Lab Scenario

As a professional ethical hacker or pen tester, your first step is to search for vulnerabilities in the target system or network using vulnerability scoring systems and databases. Vulnerability research provides awareness of advanced techniques to identify flaws or loopholes in the software that could be exploited. Using this information, you can use various tricks and techniques to launch attacks on the target system.

Lab Objectives

- Perform vulnerability research in Common Weakness Enumeration (CWE)
- Perform vulnerability research in Common Vulnerabilities and Exposures (CVE)
- Perform vulnerability research in National Vulnerability Database (NVD)

Overview of Vulnerabilities in Vulnerability Scoring Systems and Databases

Vulnerability databases collect and maintain information about various vulnerabilities present in the information systems.

The following are some of the vulnerability scoring systems and databases:

- Common Weakness Enumeration (CWE)
- Common Vulnerabilities and Exposures (CVE)
- National Vulnerability Database (NVD)
- Common Vulnerability Scoring System (CVSS)

Task 1: Perform Vulnerability Research in Common Weakness Enumeration (CWE)

Common Weakness Enumeration (CWE) is a category system for software vulnerabilities and weaknesses. It has numerous categories of weaknesses that means that CWE can be effectively employed by the community as a baseline for weakness identification, mitigation, and prevention efforts. Further, CWE has an advanced search technique with which you can search and view the weaknesses based on research concepts, development concepts, and architectural concepts.

Here, we will use CWE to view the latest underlying system vulnerabilities.

1. ☐ By default, **Windows 10** machine is selected, click [Ctrl+Alt+Delete](#) to activate the machine.

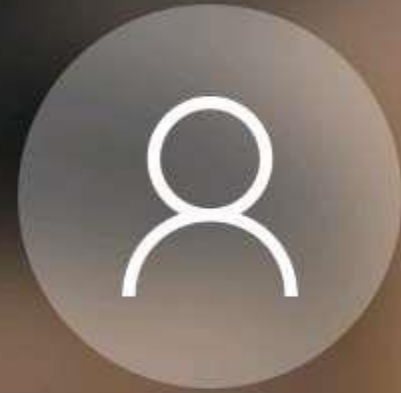
Alternatively, you can also click **Ctrl+Alt+Delete** button under **Windows 10** machine thumbnail in the **Resources** pane or Click **Ctrl+Alt+Delete** button under Commands (**thunder** icon) menu.

2. ☐ By default, **Admin** user profile is selected, click **Pa\$\$w0rd** to paste the password in the Password field and press **Enter** to login.

Alternatively, you can also click **Pa\$\$w0rd** under **Windows 10** machine thumbnail in the **Resources** pane or Click **Type Text | Type Password** button under Commands (**thunder** icon) menu.

If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.



Admin

A password input field with a white background and a thin border. It contains ten black dots representing masked characters. To the right of the dots is a small eye icon for toggling visibility, and further right is a brown button with a white right-pointing arrow.

3. ☐ Launch any browser, here, we are using **Mozilla Firefox**. In the address bar of the browser place your mouse cursor and click <https://cwe.mitre.org/> and press **Enter**
 - o If the **Default Browser** pop-up window appears, uncheck the **Always perform this check when starting Firefox** checkbox and click the **Not now** button.
 - o If a **New in Firefox: Content Blocking** pop-up window appears, follow the step and click **Got it** to finish viewing the information.
4. ☐ **CWE** website appears. In the **Google Custom Search** under **Search CWE** section, type **SMB** and click the search icon.

Here, we are searching for the vulnerabilities of the running services that were found in the target systems in previous module labs (Module 04 Enumeration).



Common Weakness Enumeration

A Community-Developed List of Software & Hardware Weakness Types

[Home](#)[About](#)[CWE List](#)[Scoring](#)[Community](#)[News](#)

CWE™ is a community-developed list of common software and hardware security weaknesses. It serves as a common language, a measuring tool for weakness identification, mitigation, and prevention efforts.

View the List of Weaknesses

[by Software Development](#)[by Hardware Design](#)[by Research Concepts](#)

Search CWE

Easily find a specific software or hardware weakness by performing a search of the CWE List by keywords(s) or by CWE-ID Number. To search, enter a space.

See the full [CWE List](#) page for enhanced information, downloads, and more.
[Submit content suggestions](#) to the CWE Team.

Total Weaknesses: [839](#)

5. ☐ The search results appear, displaying the underlying vulnerabilities in the target service (here, **SMB**). You can click any link to view detailed information on the vulnerability.

The search results might differ in your lab environment.



Common Weakness Enumeration

A Community-Developed List of Software & Hardware Weakness Types

[Home](#)[About](#)[CWE List](#)[Scoring](#)[Community](#)[News](#)

CWE™ is a community-developed list of common software and hardware security weaknesses. It serves as a common language, a measuring stick, and a resource for weakness identification, mitigation, and prevention efforts.

View the List of Weaknesses

[by Software Development](#)[by Hardware Design](#)[by Research Concepts](#)

Search CWE

Easily find a specific software or hardware weakness by performing a search of the CWE List by keywords(s) or by CWE-ID Number. To search, enter your search criteria in the space below.

About 20 results (0.11 seconds)

[CWE-200: Exposure of Sensitive Information to an Unauthorized Actor](#)

<https://cwe.mitre.org/data/definitions/200.html>

20 Feb 2020 ... There are many different kinds of mistakes that introduce information exposures. The severity of the error can range widely from low to high. The ...

[CWE-284: Improper Access Control \(4.0\) - CWE](#)

<https://cwe.mitre.org/data/definitions/284.html>

22 Feb 2020 ... Common Weakness Enumeration (CWE) is a list of common weaknesses that can be found in software and hardware.

6. ☐ Now, click any link (here, **CWE-200**) to view detailed information about the vulnerability.
7. ☐ A new webpage appears in the new tab, displaying detailed information regarding the vulnerability. You can scroll-down further to view more information.

CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Weakness ID: 200

Abstraction: Class

Structure: Simple

Presentation Filter:

▼ Description

The product exposes sensitive information to an actor that is not explicitly authorized to have access to that information.

▼ Extended Description

There are many different kinds of mistakes that introduce information exposures. The severity of the error can range wide product operates, the type of sensitive information that is revealed, and the benefits it may provide to an attacker. Some

- private, personal information, such as personal messages, financial data, health records, geographic location, or
- system status and environment, such as the operating system and installed packages
- business secrets and intellectual property
- network status and configuration
- the product's own code or internal state
- metadata, e.g. logging of connections or message headers
- indirect information, such as a discrepancy between two internal operations that can be observed by an outsider

Information might be sensitive to different parties, each of which may have their own expectations for whether the inform include:

- the product's own users
- people or organizations whose information is created or used by the product, even if they are not direct product u
- the product's administrators, including the admins of the system(s) and/or networks on which the product operates

8. ☐ Similarly, you can click on other vulnerabilities and view detailed information.
9. ☐ Now, navigate back to the **CWE** website, scroll down, and click the **CWE List** link present below the searched results.



Home

About

CWE List

Scoring

Community

News

CWE™ is a community-developed list of common software and hardware security weaknesses. It serves as a common language, a measuring stick for weakness identification, mitigation, and prevention efforts.

View the List of Weaknesses

by Software Development

by Hardware Design

by Research Concepts

Search CWE

Easily find a specific software or hardware weakness by performing a search of the CWE List by keywords(s) or by CWE-ID Number. To search, enter a space.

ENHANCED BY Google

See the full [CWE List](#) page for enhanced information, downloads, and more.
[Submit content suggestions](#) to the CWE Team.

Total Weaknesses: [839](#)

10. ☐ A new webpage appears, displaying **CWE List Version**. Scroll down, and under the **External Mappings** section, click **CWE Top 25 (2019)**.

The result might differ in your lab environment.

External Mappings

These views are used to represent mappings to external groupings such as a Top-N list, as well as to express subsets of a factor.

- CWE Top 25 (2019)
- OWASP Top Ten (2017)
- Seven Pernicious Kingdoms
- Software Fault Pattern Clusters
- SEI CERT Oracle Coding Standard for Java
- SEI CERT C Coding Standard
- SEI CERT Perl Coding Standard
- CISQ Quality Measures (2016)
- Architectural Concepts

Helpful Views

A number of additional helpful views have been created. These are based on a specific criteria and hope to provide insight

- Introduced During Design
- Introduced During Implementation
- Quality Weaknesses with Indirect Security Impacts
- Software Written in C
- Software Written in C++
- Software Written in Java

11. ☐ A webpage appears, displaying **CWE VIEW: Weaknesses in the 2019 CWE Top 25 Most Dangerous Software Errors**. Scroll down and view a list of **Weaknesses in the 2019 CWE Top 25 Most Dangerous Software Errors** under the **Relationships** section. You can click on each weakness to view detailed information on it.

This information can be used to exploit the vulnerabilities in the software and further launch attacks.

The result publishing year be might different in your lab environment.

[Expand All](#) | [Collapse All](#)

1200 - Weaknesses in the 2019 CWE Top 25 Most Dangerous Software Errors

- Improper Restriction of Operations within the Bounds of a Memory Buffer - (119)
- Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') - (79)
- Improper Input Validation - (20)
- Exposure of Sensitive Information to an Unauthorized Actor - (200)
- Out-of-bounds Read - (125)
- Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') - (89)
- Use After Free - (416)
- Integer Overflow or Wraparound - (190)
- Cross-Site Request Forgery (CSRF) - (352)
- Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') - (22)
- Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') - (78)
- Out-of-bounds Write - (787)
- Improper Authentication - (287)
- NULL Pointer Dereference - (476)
- Incorrect Permission Assignment for Critical Resource - (732)
- Unrestricted Upload of File with Dangerous Type - (434)
- Improper Restriction of XML External Entity Reference - (611)
- Improper Control of Generation of Code ('Code Injection') - (94)
- Use of Hard-coded Credentials - (798)
- Uncontrolled Resource Consumption - (400)
- Missing Release of Resource after Effective Lifetime - (772)
- Untrusted Search Path - (426)
- Deserialization of Untrusted Data - (502)
- Improper Privilege Management - (269)
- Improper Certificate Validation - (295)

▼ References

[REF-1028] "2019 CWE Top 25 Most Dangerous Software Errors". 2019-09-16. <<http://cwe.mitre.org/top25/archive/2019/2>>

▼ View Metrics

12. ☐ Similarly, you can go back to the CWE website and explore other options, as well.
 13. ☐ This concludes the demonstration of checking vulnerabilities in the Common Weakness Enumeration (CWE).
 14. ☐ Close all open windows and document all the acquired information.
-

Task 2: Perform Vulnerability Research in Common Vulnerabilities and Exposures (CVE)

Common Vulnerabilities and Exposures (CVE) is a publicly available and free-to-use list or dictionary of standardized identifiers for common software vulnerabilities and exposures. It is used to discuss or share information about a unique software or firmware vulnerability, provides a baseline for tool evaluation, and enables data exchange for cybersecurity automation.

Here, we will use CVE to view the latest underlying system and software vulnerabilities.

1. ☐ In **Windows 10** machine, launch any browser (here, **Mozilla Firefox**). In the address bar of the browser place your mouse cursor and click <https://cve.mitre.org/> and press **Enter**
2. ☐ **CVE** website appears. In the right pane, under the **Newest CVE Entries** section, recently discovered vulnerabilities are displayed.

The results might differ in your lab environment.



CVE® is a [list](#) of entries—each containing an identification number, a description, and at least one public reference—for publicly known cybersecurity vulnerabilities. CVE Entries are used in numerous cybersecurity [products and services](#) from around the world, including the U.S. National Vulnerability Database ([NVD](#)).

Latest CVE News

- [CVE Board Charter Updated to Version 3.2](#)
- [Xiaomi Added as CVE Numbering Authority \(CNA\)](#)
- [GitLab Added as CVE Numbering Authority \(CNA\)](#)

[More News >>](#)

CVE Blog

CVE Program Report for Calendar Year Q1-2020 Now Available

[CY Q1-2020 Milestones](#) - CVE Numbering Authorities (CNAs), CVE Board, CVE Working Groups, and more
[CY Q1-2020 Metrics](#) - CVE Entries and requests for CVE IDs from the CVE Program Root CNA

Become a CNA

[CVE Numbering Authorities](#), or “CNAs,” are essential to the CVE Program’s success and every [CVE Entry](#) is added to the [CVE List](#) by a CNA.

Join today!

- [Business benefits](#)
- [No fee or contract](#)
- [Few requirements](#)
- [Easy to join](#)

Total CNAs: [128](#) | Total Countries: [21](#)



[Learn How to Become a CNA >>>](#)

[Watch CNA Onboarding Videos >>](#)

3. ☐ You can copy the name of any vulnerability under the **Newest CVE Entries** section and search on CVE to view detailed information on it. (here, we are selecting the vulnerability **CVE-2020-13910**)
4. ☐ Now, click on the **Search CVE List** tab. Under **Search CVE List** section, type the vulnerability name (here, **CVE-2020-4051**) in the search bar, and click **Submit**.



Common Vulnerabilities and Exposures

CVE List ▾

CNAs ▾

WGs ▾

Board ▾

About ▾

Search CVE List

Download CVE


Data Feeds

HOME > CVE LIST > SEARCH CVE LIST

Search CVE List

You can search the CVE List for a [CVE Entry](#) if the [CVE ID](#) is known. To search by keyword, use a specific term or multiple keywords. Search results will be the relevant CVE Entries.

View the [search tips](#).

5.  **Search Results** page appears, displaying the information regarding the searched vulnerability. You can click the vulnerability link to view further detailed information regarding the vulnerability.



Common Vulnerabilities and Exposures

[CVE List](#) ▾

[CNAs](#) ▾

[WGs](#) ▾

[Board](#) ▾

[About](#) ▾

[Search CVE List](#)

[Download CVE](#)

[Data Feeds](#)

[HOME](#) > [CVE](#) > [SEARCH RESULTS](#)

Search Results

There are **1** CVE entries that match your search.

Name	Description
CVE-2020-4051	In Dijit before versions 1.11.11, and greater than or equal to 1.12.0 and less than 1.12.9, and greater than or equal to 1.13.0 to 1.14.0 and less than 1.14.7, and greater than or equal to 1.15.0 and less than 1.15.4, and greater than or equal to 1.16.0 scripting vulnerability in the Editor's LinkDialog plugin. This has been fixed in 1.11.11, 1.12.9, 1.13.8, 1.14.7, 1.15.4, 1.16.3.

SEARCH CVE USING KEYWORDS:

[Submit](#)

You can also search by reference using the [CVE Reference Maps](#).
For More Information: [CVE Request Web Form](#) (select "Other" from dropdown)

6. ☐ Similarly, in the **Search CVE List** section, you can search for a service-related vulnerability by typing the service name (here, **SMB**) and click **Submit**.

You can search for the vulnerabilities of the running services that were found in the target systems in previous module labs (Module 04 Enumeration).



Common Vulnerabilities and Exposures

CVE List ▾

CNAs ▾

WGs ▾

Board ▾

About ▾

Search CVE List

Download CVE

Data Feeds

HOME > CVE LIST > SEARCH CVE LIST

Search CVE List

You can search the CVE List for a [CVE Entry](#) if the [CVE ID](#) is known. To search by keyword, use a specific term or multiple keywords. Search results will be the relevant CVE Entries.

View the [search tips](#).

7. ☐ **Search Results** page appears, displaying a list of vulnerabilities in the target service (**SMB**) along with their description, as shown in the screenshot.

The results might vary in your lab environment.



Common Vulnerabilities and Exposures

CVE List

CNAs

WGs

Board

About

Search CVE List

Download CVE

Data Feeds

HOME > CVE > SEARCH RESULTS

Search Results

There are 442 CVE entries that match your search.

Name	Description
CVE-2020-9324	Aquaforest TIFF Server 4.0 allows Unauthenticated SMB Hash Capture via UNC.
CVE-2020-6963	In ApexPro Telemetry Server Versions 4.2 and prior, CARESCAPE Telemetry Server v4.2 & prior, Clinical Information Center Station (CSCS) Versions 1.X, the affected products utilized hard coded SMB credentials, which may allow an attacker to re
CVE-2020-2578	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Kernel). The supported version that is affected i unauthenticated attacker with network access via SMB to compromise Oracle Solaris. While the vulnerability is in Oracle So products. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (parti 5.8 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:L).
CVE-2020-2558	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Kernel). The supported version that is affected i unauthenticated attacker with network access via SMB to compromise Oracle Solaris. While the vulnerability is in Oracle So products. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (parti 5.8 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:L).
CVE-2020-1301	A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 1.0 (SMBv1) server handl Code Execution Vulnerability'.
CVE-2019-9565	Druide Antidote RX, HD, 8 before 8.05.2287, 9 before 9.5.3937 and 10 before 10.1.2147 allows remote attackers to steal upon a direct launch of the product, or upon an indirect launch via an integration such as Chrome, Firefox, Word, Outlook, to access a share with the PLUG-INS subdomain name; an attacker may be able to use Active Directory Domain Services t
CVE-2019-7097	Adobe Dreamweaver versions 19.0 and earlier have an insecure protocol implementation vulnerability. Successful exploitati request is subject to a relay attack.
CVE-2019-6452	Kyocera Command Center RX TASKalfa4501i and TASKalfa5052ci allows remote attackers to abuse the Test button in the

8. ☐ Further, you can click on **CVE-ID** of any vulnerability to view its detailed information. Here, we will click on the first CVE-ID link.
9. ☐ Detailed information regarding the vulnerability is displayed such as its **Description**, **References**, and **Date Entry Created**. Further, you can click on links under the **References** section to view more information on the vulnerability.



Common Vulnerabilities and Exposures

CVE List ▾

CNAs ▾

WGs ▾

Board ▾

About ▾

Search CVE List

Download CVE

Data Feeds

HOME > CVE > CVE-2020-9324

CVE-ID

CVE-2020-9324

[Learn more at National Vulnerability Database \(NVD\)](#)

• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

Aquaforest TIFF Server 4.0 allows Unauthenticated SMB Hash Capture via UNC.

References

Note: [References](#) are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- MISC: https://www.aquaforest.com/en/release_history.asp
- MISC: <https://www.criticalstart.com/multiple-vulnerabilities-discovered-in-tiff-server-from-aquaforest/>
- MISC: <https://www.criticalstart.com/resources/>

Assigning CNA

MITRE Corporation

Date Entry Created

20200220

Disclaimer: The [entry creation date](#) may reflect when the CVE ID was allocated or reserved, and does not necessarily reflect when the vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

10. ☐ Likewise, you can search for other target services for the underlying vulnerabilities in the **Search CVE List** section.
 11. ☐ This concludes the demonstration of checking vulnerabilities in the Common Vulnerabilities and Exposures (CVE).
 12. ☐ Close all open windows and document all the acquired information.
-

Task 3: Perform Vulnerability Research in National Vulnerability Database (NVD)

The National Vulnerability Database (NVD) is the U.S. government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP). These data enable the automation of vulnerability management, security measurement, and compliance. The NVD includes databases of security checklist references, security-related software flaws, misconfigurations, product names, and impact metrics.

Here, we will use the NVD to view the latest underlying system and software vulnerabilities.

1. ☐ In **Windows 10** machine, launch any browser (here, **Mozilla Firefox**). In the address bar of the browser place your mouse cursor and click <https://nvd.nist.gov/> and press **Enter**
2. ☐ **NATIONAL VULNERABILITY DATABASE** website appears: the recently discovered vulnerabilities can be viewed.
3. ☐ You can click on the CVE-ID link (here, **CVE-2020-6269**) to view detailed information about the vulnerability.

The results might differ in your lab environment.



Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

General



Vulnerabilities



Vulnerability Metrics



Products



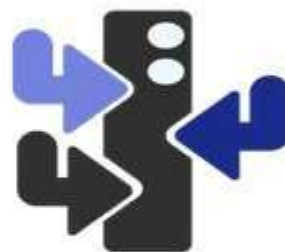
Configurations (CCE)

Contact NVD

Other Sites



Search



**CVSS/CWE from CVE List
now Supported!**



**CVSS Version 3.1 Official
Support!**

The NVD is the U.S. government repository of standards based vulnerability management data managed by the U.S. Department of Homeland Security. This data enables automation of vulnerability management, security-related software flaws, misconfigurations, and security checklist references. This data is available through the Security Automation Protocol (SCAP). This data enables automation of vulnerability management, security-related software flaws, misconfigurations, and security checklist references.

4. ☐ A new webpage appears, displaying **CVE-2020-6269 Detail**. You can view detailed information such as **Current Description**, **Severity**, **References**, and **Weakness Enumeration**.
5. ☐ Under the **Severity** section, click the **Base Score** link to view the CVSS details regarding the vulnerability.

CVE-2020-6269 Detail

Current Description

Under certain conditions SAP Business Objects Business Intelligence Platform, version 4.2, allows an attacker to access information which would otherwise be restricted, leading to Information Disclosure.

Source: MITRE

[+View Analysis Description](#)

Severity

CVSS Version 3.x

CVSS Version 2.0

CVSS 3.x Severity and Metrics:



NIST: NVD

Base Score: 6.5 MEDIUM

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



CNA: SAP SE

Base Score: 4.3 MEDIUM

Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or

6. ☐ A new webpage appears, displaying information such as **Base Scores**, **Temporal Score**, and **Environmental Score Overall Score** related to a vulnerability in graphical form, under **Common Vulnerability Scoring System Calculator CVE-2020-6269**.
- o **Base Score:** The metric most relied upon by enterprises and deals with the inherent qualities of a vulnerability. The table below describes the severity of a vulnerability depending upon the Base Score range:

CVSS v3.0 Ratings

Severity	Base Score Range
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

CVSS v2.0 Ratings

Severity	Base Score Range
Low	0.0-3.9
Medium	4.0-6.9
High	7.0-10

[more...](#)

- o **Temporal Score:** Represents the qualities of the vulnerability that change over time, and the Environmental score represents the qualities of the vulnerability that are specific to the affected user's environment.
- o **Overall Score:** Sum total of both the scores (CVSS Base Score, CVSS Temporal Score).

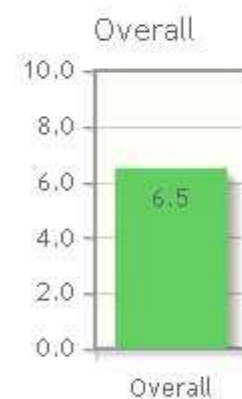
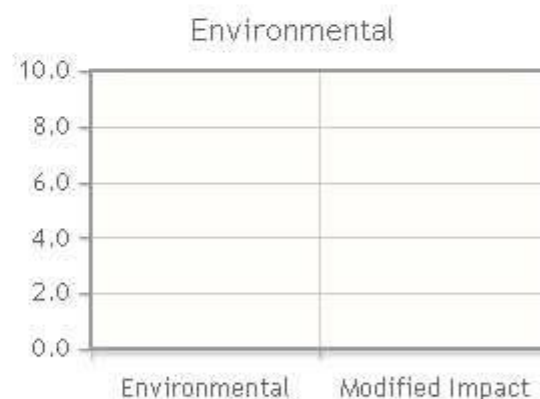
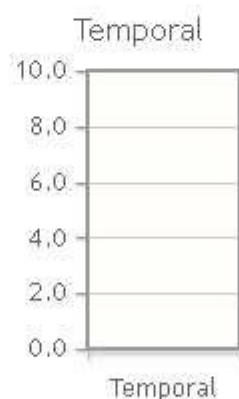
CVSS Version 3.0

CVSS Version 3.1

Common Vulnerability Scoring System Calculator CVE-2020-6269

Source: NIST

This page shows the components of the CVSS score for example and allows you to refine the CVSS base standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Overall Score.



CVSS v3.1 Vector

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

7. ☐ Scroll down to view more detailed information on different score metrics such as **Base Score Metrics**, **Temporal Score Metrics**, and **Environmental Score Metrics**.

The results might differ depending upon the selected vulnerability

Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*

Network (AV:N)

Adjacent Network (AV:A)

Local (AV:L)

Physical (AV:P)

Attack Complexity (AC)*

Low (AC:L)

High (AC:H)

Privileges Required (PR)*

None (PR:N)

Low (PR:L)

High (PR:H)

User Interaction (UI)*

None (UI:N)

Required (UI:R)

Scope (S)*

Unchanged (S:U)

Changed (S:C)

Impact Metrics

Confidentiality Impact (C)*

None (C:N)

Low (C:L)

High (C:H)

Integrity Impact (I)*

None (I:N)

Low (I:L)

High (I:H)

Availability Impact (A)*

None (A:N)

Low (A:L)

High (A:H)

* - All base metrics are required to generate a base score.

Temporal Score Metrics

Exploitability (E)

Not Defined (E:X)

Unproven that exploit exists (E:U)

Proof of concept code (E:P)

Functional exploit exists (E:F)

High (E:H)

Remediation Level (RL)

Not Defined (RL:X)

Official fix (RL:O)

Temporary fix (RL:T)

Workaround (RL:W)

Unavailable (RL:U)

Report Confidence (RC)

Not Defined (RC:X)

Unknown (RC:U)

Reasonable (RC:R)

Confirmed (RC:C)

Environmental Score Metrics

Base Modifiers

Attack Vector (AV)

Not Defined (MAV:X) Network (MAV:N) Adjacent Network (MAV:A)

Local (MAV:L) Physical (MAV:P)

Attack Complexity (AC)

Not Defined (MAC:X) Low (MAC:L) High (MAC:H)

Privileges Required (PR)

Not Defined (MPR:X) None (MPR:N) Low (MPR:L) High (MPR:H)

User Interaction (UI)

Not Defined (MUI:X) None (MUI:N) Required (MUI:R)

Scope (S)

Not Defined (MS:X) Unchanged (MS:U) Changed (MS:C)

Clear Form

Impact Metrics

Confidentiality Impact (C)

Not Defined (MC:X) None (MC:N) Low (MC:L)

High (MC:H)

Integrity Impact (I)

Not Defined (MI:X) None (MI:N) Low (MI:L)

High (MI:H)

Availability Impact (A)

Not Defined (MA:X) None (MA:N) Low (MA:L)

High (MA:H)

8.  Now, navigate back to the main page of the **NATIONAL VULNERABILITY DATABASE** website. Expand **Vulnerabilities** and click **Search & Statistics** option, as shown in the screenshot.



Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

General



Vulnerabilities



[Search & Statistics](#)

[Full Listing](#)

[Categories](#)

[Data Feeds](#)

[Vendor Comments](#)

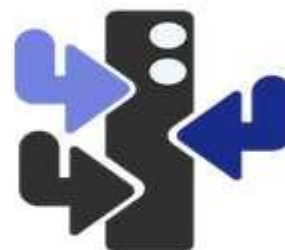
Vulnerability Metrics



Products



Configurations (CCE)



**CVSS/CWE from CVE List
now Supported!**



**CVSS Version 3.1 Official
Support!**

The NVD is the U.S. government repository of standards based vulnerability management data managed by the U.S. Department of Homeland Security. This data enables automation of vulnerability management, security scanning, and incident response. The NVD also includes databases of security checklist references, security-related software flaws, misconfigurations, and other security-related information.

9. ☐ **Search Vulnerability Database** page appears. In the **Keyword Search** field, type a target service (here, **SMB**) to find vulnerabilities associated with it and click **Search**.

You can search for the vulnerabilities of the running services that were found in the target systems in previous module labs (Module 04 Enumeration).



Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

VULNERABILITIES

Search Vulnerability Database

Try a product name, vendor name, CVE name, or an OVAL query.

NOTE: Only vulnerabilities that match ALL keywords will be returned, Linux kernel vulnerabilities are categorized separately from vulnerabilities in

Search Type

☒ Basic ☐ Advanced

Results Type

☒ Overview ☐ Statistics

Keyword Search

Contains HyperLinks

- ☐ US-CERT Technical Alerts
- ☐ US-CERT Vulnerability Notes
- ☐ OVAL Queries

Search

Reset

10. ☐ The **Search Results** page appears, displaying detailed information on the underlying vulnerabilities in the target service.
11. ☐ You can further view detailed information on each vulnerability by clicking on the **Vuln ID** link.

Search Results (Refine Search)

Sort r

Search Parameters:

- Results Type: Overview
- Keyword (text search): SMB
- Search Type: Search All

There are **416** matching records.Displaying matches **1** through **20**.

Vuln ID

Summary

CVE-2020-1301

A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain 'Windows SMB Remote Code Execution Vulnerability'.

Published: June 09, 2020; 04:15:19 PM -04:00**CVE-2020-1284**

A denial of service vulnerability exists in the way that the Microsoft Server Message Block 3.1.1 (SMBv3) protocol handles certain 'Windows SMBv3 Client/Server Denial of Service Vulnerability'.

Published: June 09, 2020; 04:15:18 PM -04:00**CVE-2020-1206**

An information disclosure vulnerability exists in the way that the Microsoft Server Message Block 3.1.1 (SMBv3) protocol handles certain 'Windows SMBv3 Client/Server Information Disclosure Vulnerability'.

Published: June 09, 2020; 04:15:13 PM -04:00**CVE-2020-9324**

Aquaforest TIFF Server 4.0 allows Unauthenticated SMB Hash Capture via UNC.

Published: March 18, 2020; 10:15:17 AM -04:00

12. ☐ Likewise, you can search for other target services for the underlying vulnerability in the **Search Vulnerability Database** section.
13. ☐ This concludes the demonstration of checking vulnerabilities in the National Vulnerability Database (NVD).
14. ☐ Close all open windows and document all the acquired information.