About CVSS

What is CVSS?

CVSS is the Common Vulnerability Scoring System, an open framework for communicating about computer security vulnerabilities maintained by the Forum of Incident Response and Security Teams. It is used by, among others, the National Vulnerability Database and the National Institute of Standards and Technology in the US. It uses a numerical score describing how severe a vulnerability is considered to be and a coded vector describing the nature of the vulnerability in question.

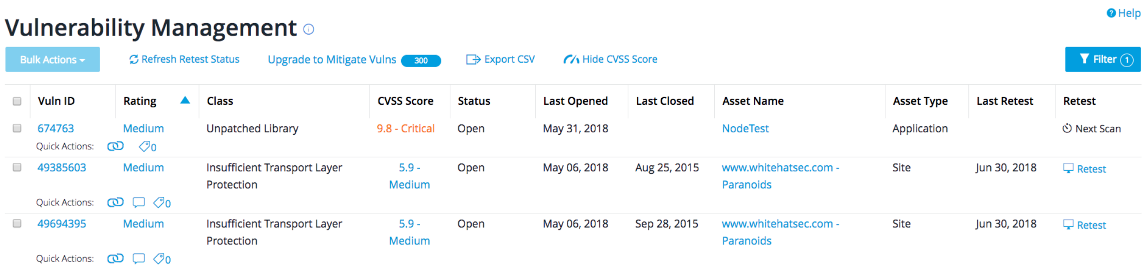
Managing, prioritizing, and fixing vulnerabilities is top priority for security teams. However, because different vendors are focused on different parts of the IT infrastructure, they often utilize different rating systems to describe the importance of those vulnerabilities. This makes it difficult for organizations to compare and prioritize vulnerabilities across the entire infrastructure.

The Common Vulnerability Scoring System (CVSS) overcomes that challenge by using a single common vulnerability scoring system across the entire IT stack. In CVSS v3, complexity, privilege, and user interaction are all associated to a particular vulnerable component, along with confidentiality, integrity and availability needs. That means that if a feature in component A is terribly vulnerable, and it makes a bad thing happen in component B, the CVSS rating system will measure the end-to-end vulnerability score. In addition, it's now possible for you to customize your base CVSS score based on your own internal IT security risk profile.

The CVSS Score has three components: the Base, Temporal, and Environmental metrics. The Base metric measures intrinsic aspects of the vulnerability -- primarily how easy it is to take advantage of it and what kind of damage can be done if it is exploited. This value is set by WhiteHat based on the CVSS guidelines. The Environmental metric reflects the specific circumstances applicable to this asset, and can be modified by the customer as part of a Vuln Policy or for a specific instance of a vulnerability. The Temporal metric reflects the maturity level of the exploit and the remediation that is available, if any.

The CVSS Base and Environmental Score (as a total) can be displayed on your vuln detail pages: in the Findings tab, click on "Show CVSS," or click on "Hide CVSS" to turn the display off; in the Attack Vector Detail Report and Vuln Detail Report turn on the option to show the CVSS Score in the report generation screen.

Findings Tab

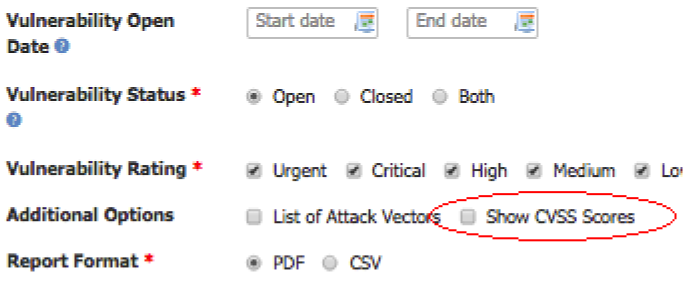


Vulnerability Management

☐	Vuln ID	Rating	Class	CVSS Score	Status	Last Opened	Last Closed	Asset Name	Asset Type	Last Retest	Retest
☐	674763	Medium	Unpatched Library	9.8 - Critical	Open	May 31, 2018		NodeTest	Application		Next Scan
☐	49385603	Medium	Insufficient Transport Layer Protection	5.9 - Medium	Open	May 06, 2018	Aug 25, 2015	www.whitehatsec.com - Paranoids	Site	Jun 30, 2018	Retest
☐	49694395	Medium	Insufficient Transport Layer Protection	5.9 - Medium	Open	May 06, 2018	Sep 28, 2015	www.whitehatsec.com - Paranoids	Site	Jun 30, 2018	Retest

Report Generation

CVSS Scores can be included in the Vuln Detail Report for Sites or in the Attack Vector Detail Report. Select Assets, Sites, or Groups for these reports and make sure that the "CVSS" checkbox in "Additional Options" is checked:



Vulnerability Open Date	Start date End date
Vulnerability Status *	● Open ○ Closed ○ Both
Vulnerability Rating *	☑ Urgent ☑ Critical ☑ High ☑ Medium ☑ Lo
Additional Options	☐ List of Attack Vectors ☐ Show CVSS Scores
Report Format *	● PDF ○ CSV

Reports generated will now include the CVSS Scores.

How Does CVSS Work?

The CVSS score is calculated in two parts: a Base CVSS score, which is primarily determined by the vulnerability itself -- what access is required to exploit it, what kind of damage can it do -- and an Environmental CVSS score, which considers the asset that has the vulnerability and what the needs of that asset are for confidentiality, integrity, and availability, and can consider modifications that may affect how easy it is to exploit the vulnerability in this specific case.

Please see "CVSSv3 Factors" for a deeper understanding of the factors used to calculate CVSS scores and the effect of various changes; you can also go to https://www.first.org/cvss/calculator/3.0 to explore how changes to these values affect the CVSS scores.

The Common Vulnerability Scoring System (CVSS)

Understanding the CVSS Base Score

The Base CVSS Score is calculated based on:

- AV: Access Vector (requires physical presence, requires local access, requires access to an adjacent network, or requires network access)
- AC: Attack Complexity (low or high)
- PR: Privileges required (none, low, or high)
- UI: User Interaction (none or required)
- S: Scope (the exploit can affect resources beyond the intention of the vulnerable component (changed), or it cannot (unchanged))
- C: Confidentiality requirement for the asset (none, low, or high)
- I: Integrity requirement for the asset (none, low, or high)
- A: Availability requirement for the asset (none, low, or high)

Understanding the CVSS Environmental Score

The Environmental CVSS Score is calculated based on the impact the vulnerability could have on Confidentiality, Integrity, and Availability of the system (none, low, or high) and on modifications of the base factors (Modified Attack Vector, Modified Attack Complexity, Modified Privileges Required, Modified User Interaction, Modified Scope, Modified Confidentiality, Modified Integrity, Modified Availability -- shown in the vector string as MAV, MAC, MPR, MUI, MS, MC, MI, and MA). These values can be set by your Sentinel Administrator to reflect your specific circumstances.

CVSS Vector String

When these factors are all defined, they will create a Vector String that provides this information in a compressed format. The Vector String begins with the CVSS version being used, and then each factor is represented by an abbreviation followed by a colon and the value for this particular vulnerability, and the factors are separated by forward slashes. For example:

CVSS:3.0/AV:L/AC:H/PR:l/UI:N/S:C/C:L/I:L/A:L/CR:H/IR:H/AR:L/MAV:L/MAC:H/MPR:H/MUI:N/MS:U/MC:L/MI:L/MA:L

That vector string says that in the CVSS v. 3.0 scoring system, for this vulnerability, the Attack Vector is local, the Attack Complexity is high, the Privileges Required are low, the User Interaction required is none, the Scope can be changed, the Confidentiality risk is low, the Integrity risk is low, and the availability risk is low. In addition, this string shows the Environmental data. The confidentiality requirement for this asset is high, the integrity requirement is high, the availability requirement is low, and the Modified attack vector, complexity, etc. are local, high, high, none, changed, low, low, and low. (You can see the CVSSv3 Vector by clicking on the CVSS score shown on the Findings tab. The Vector will reflect any value that has been set for this vulnerability.)

These values will result in a Base CVSS score of Medium, and an Environmental score that is also Medium. More details are available at https://www.first.org/cvss/calculator/3.0, where you can also see the results of possible changes.