

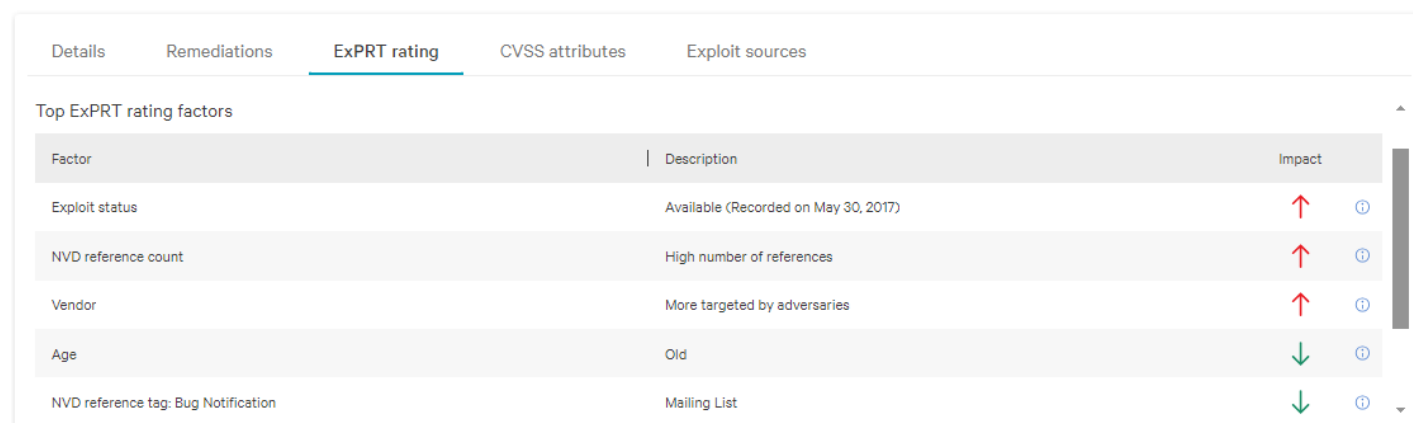
## CrowdStrike Vulnerability Management

The vulnerability management tool in CrowdStrike provides valuable insight into outdated OS, vulnerable software, and other potential misconfigurations on your managed assets. Remediating these vulnerabilities is an important step towards keeping your assets protected – the CrowdStrike sensor does a great job at blocking and quarantining malicious activity, but if you can prevent attempts from happening in the first place by keeping your assets up to date then in many ways that’s even better! This document will discuss topics to help you get the most out of Vulnerability Management.

### ExPRT rating

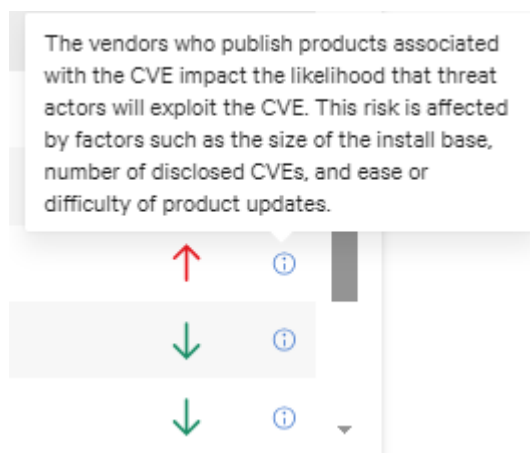
Most of us are probably familiar with the standard CVSS (Common Vulnerability Scoring System) for rating vulnerabilities. This system rates a vulnerability from 0 to 10 based on factors like the potential impact and ease of exploitation. **ExPRT** is CrowdStrike’s own rating system which improves on CVSS by incorporating multiple data sources (including CrowdStrike’s own threat intelligence), dynamically rating updates based on new information, and increasing transparency to show which factors are impacting a vulnerability’s rating. These improvements help provide a more complete picture of the actual risk to your organization and help you decide which vulnerabilities or assets need immediate attention.

In *Exposure management > Vulnerability management > Vulnerabilities*, select a vulnerability to open the details page. From there you can access tabs to show which of your assets are vulnerable, how to remediate, and links to vendor information. If you click on the ‘ExPRT rating’ tab you can view the rating factors that caused CrowdStrike to adjust the severity of this vulnerability.



Factor	Description	Impact
Exploit status	Available (Recorded on May 30, 2017)	↑ ⓘ
NVD reference count	High number of references	↑ ⓘ
Vendor	More targeted by adversaries	↑ ⓘ
Age	Old	↓ ⓘ
NVD reference tag: Bug Notification	Mailing List	↓ ⓘ

Most vulnerabilities will have multiple factors that increase or decrease the impact, and CrowdStrike aggregates that data to come up with their final ExPRT rating (though as mentioned, it is dynamic and can change in the future if new information comes to light so nothing is ever really ‘final’). Hovering over the ‘i’ icon on the right side will provide more information on each rating factor.

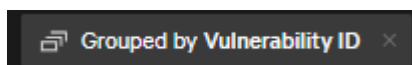


MCNC recommends taking ExPRT rating information into heavy consideration when evaluating the severity of vulnerabilities in your environment, as the information provided by CrowdStrike is likely to be much more up to date than CVSS data found in most vulnerability advisories.

## Grouping

Depending on how many assets are in your CrowdStrike environment there could be hundreds or thousands of open vulnerabilities, making individual review difficult if not impossible. CrowdStrike allows you to group vulnerabilities by parameters like Asset, Product, or Remediation, making it much easier to see which of your assets, OS, or software needs the most attention.

In *Vulnerability management* > *Vulnerabilities*, locate the ‘Grouped by’ option on the right side.



By changing this to ‘Grouped by Asset’ you can now see a sorted list of the assets in your environment with the most open vulnerabilities, including Criticals and vulnerabilities with actively used exploits. This can help you track down assets that either aren’t receiving the same patches as other assets or may have an uncommon piece of software with a large number of vulnerabilities. Clicking on the asset will open a new page that allows you to see the full vulnerability list as well as recommended remediations.

Vulnerabilities  
Total vulnerabilities

1.9K

Remediations  
Total recommended

47

Installed patches  
Last patch confirmed

Jan. 2, 2024

**Vulnerabilities** 1.9K items | [Go to full table](#)

CVE ID Exploit status ExPRT rating Platform Status: 1 excluded Suppression status: 1 applied Vendor & product Add/remove filters + Reset all

Vulnerability ID	ExPRT rating	CVSS severity	Exploit status	Remediation	Vulnerable product versions
CVE-2024-26162	High	High	Unproven	Install patch for Microsoft Windo...	Windows Server 2016 1607
CVE-2024-21438	Medium	High	Unproven	Install patch for Microsoft Windo...	Windows Server 2016 1607
CVE-2024-26159	High	High	Unproven	Install patch for Microsoft Windo...	Windows Server 2016 1607
CVE-2024-26197	Low	Medium	Unproven	Install patch for Microsoft Windo...	Windows Server 2016 1607

You can also group by Product or Remediation (since the remediation is almost always going to be something like ‘Update this product’, these two options give similar results). This allows you to see the OS or software with the most open vulnerabilities in your environment, allowing you to prioritize your patching effort to have the most positive impact.

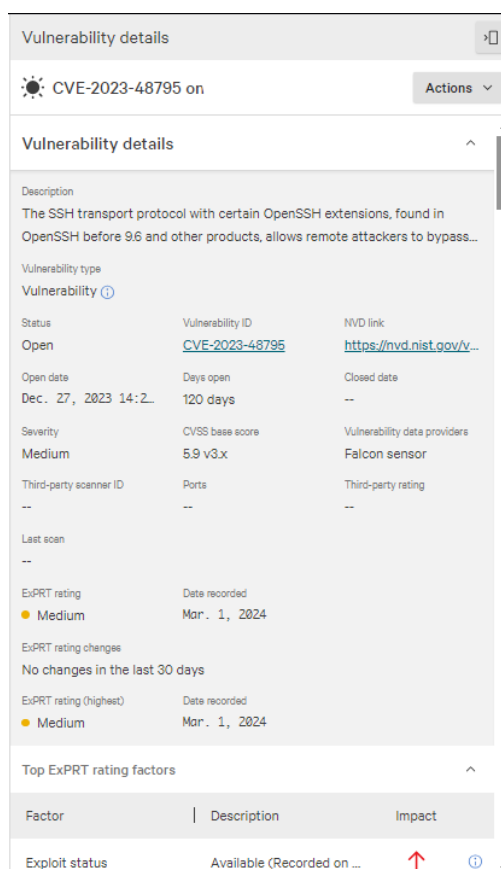
Remediation	Description	Vulnerabilities
<a href="#">Update Microsoft Windows Server 2016</a>	Install patch for Microsoft Windows Server 2016 14393 (Server): S...	4,624
<a href="#">Update Google Chrome Enterprise</a>	Update Google Chrome Enterprise to version 124.0.6367.78 or newer	3,901
<a href="#">Update Mozilla Firefox</a>	Update Mozilla Firefox to version 125.0 or newer	3,393
<a href="#">Update Microsoft Windows Server 2019</a>	Install patch for Microsoft Windows Server 2019 17763 (Server): Se...	2,799
<a href="#">Update Apple Mac OS 12</a>	Update Apple Mac OS 12 to version 14.0 or newer	1,857
<a href="#">Update Apple Mac OS 13</a>	Update Apple Mac OS 13 to version 14.0 or newer	1,615

Grouping can be used in conjunction with the filter bar, allowing you to do things like find which assets have the most critical vulnerabilities or which remediations will close the most vulnerabilities with actively used exploits on assets in your ‘Linux Server’ host group.

## Vulnerability Evidence

One feature CrowdStrike has added recently is the ability to view Vulnerability evidence. This allows you to see exactly which check CrowdStrike has used to determine the presence of a vulnerability on a particular asset, which can be helpful if you believe you’ve already patched or are otherwise unsure what a vulnerability indicates.

In *Vulnerability Management*, select a vulnerability ID, asset, or remediation you’d like to investigate. This opens the details page which provides a full list of vulnerabilities that fit the criteria. Clicking on an individual vulnerability opens up the Vulnerability details tab, showing you all available information about a vulnerability.



Vulnerability details

CVE-2023-48795 on Actions

### Vulnerability details

Description  
The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass...

Vulnerability type  
Vulnerability ⓘ

Status	Vulnerability ID	NVD link
Open	<a href="#">CVE-2023-48795</a>	<a href="https://nvd.nist.gov/v...">https://nvd.nist.gov/v...</a>
Open date	Days open	Closed date
Dec. 27, 2023 14:2...	120 days	--
Severity	CVSS base score	Vulnerability data providers
Medium	5.9 v3.x	Falcon sensor
Third-party scanner ID	Ports	Third-party rating
--	--	--
Last scan		
--		
ExPRT rating	Date recorded	
● Medium	Mar. 1, 2024	
ExPRT rating changes		
No changes in the last 30 days		
ExPRT rating (highest)	Date recorded	
● Medium	Mar. 1, 2024	

### Top ExPRT rating factors

Factor	Description	Impact
Exploit status	Available (Recorded on ...	↑ ⓘ

Scrolling down to ‘Affected product versions and Vulnerability evidence’ allows you to see the available evidence and view all test results.

Notable tests 2 Items

Title	Type																				
<ul style="list-style-type: none"> <li>Check if the lower version of FileZilla is less than 3.66.4</li> </ul> <p><b>Existence check:</b> At least one exists <b>Comparison check:</b> All items must match</p> <table border="1"> <thead> <tr> <th>Hive</th> <th>Key</th> <th>Name</th> <th>Windows view</th> <th>Value</th> <th>Type</th> <th>Tested proper...</th> <th>Actual</th> <th>Operation</th> <th>Expected value</th> </tr> </thead> <tbody> <tr> <td>HKEY_LOCAL...</td> <td>SOFTWARE\...</td> <td>DisplayVersion</td> <td>32_bit</td> <td>3.60.1</td> <td>reg_sz</td> <td>value</td> <td>3.60.1</td> <td>less than</td> <td>3.66.4</td> </tr> </tbody> </table> <p>1 result (1-1 shown)   Items per page 50   Page 1 of 1</p>	Hive	Key	Name	Windows view	Value	Type	Tested proper...	Actual	Operation	Expected value	HKEY_LOCAL...	SOFTWARE\...	DisplayVersion	32_bit	3.60.1	reg_sz	value	3.60.1	less than	3.66.4	Registry item
Hive	Key	Name	Windows view	Value	Type	Tested proper...	Actual	Operation	Expected value												
HKEY_LOCAL...	SOFTWARE\...	DisplayVersion	32_bit	3.60.1	reg_sz	value	3.60.1	less than	3.66.4												
<ul style="list-style-type: none"> <li>Check if the lower version of FileZilla is greater than or equal to 3.0.0</li> </ul> <p><b>Existence check:</b> At least one exists <b>Comparison check:</b> All items must match</p> <table border="1"> <thead> <tr> <th>Hive</th> <th>Key</th> <th>Name</th> <th>Windows view</th> <th>Value</th> <th>Type</th> <th>Tested proper...</th> <th>Actual</th> <th>Operation</th> <th>Expected value</th> </tr> </thead> <tbody> <tr> <td>HKEY_LOCAL...</td> <td>SOFTWARE\...</td> <td>DisplayVersion</td> <td>32_bit</td> <td>3.60.1</td> <td>reg_sz</td> <td>value</td> <td>3.60.1</td> <td>greater than ...</td> <td>3.0.0</td> </tr> </tbody> </table> <p>1 result (1-1 shown)   Items per page 50   Page 1 of 1</p>	Hive	Key	Name	Windows view	Value	Type	Tested proper...	Actual	Operation	Expected value	HKEY_LOCAL...	SOFTWARE\...	DisplayVersion	32_bit	3.60.1	reg_sz	value	3.60.1	greater than ...	3.0.0	Registry item
Hive	Key	Name	Windows view	Value	Type	Tested proper...	Actual	Operation	Expected value												
HKEY_LOCAL...	SOFTWARE\...	DisplayVersion	32_bit	3.60.1	reg_sz	value	3.60.1	greater than ...	3.0.0												

Here you can see results for notable and full tests that the sensor has used to determine the presence of a particular vulnerability. In the above screenshot we can see that Crowdstrike was able to detect an installed version of Filezilla within the range that is impacted by the OpenSSH vulnerability based on visibility into this asset’s registry. If we look back at the details for this vulnerability we can also see that it matches the information above by recommending Filezilla be updated to version 3.67.0.

### Remediation details 1 ^

Description	Vulnerabilities
<a href="#">Update FileZilla to version 3.67.0 or newer</a>	1

[See all remediations](#)