How to Read Your Security Score - Detected Common Vulnerabilities & Exploits (CVEs)

https://campus.barracuda.com/doc/98211821/

The **Detected Common Vulnerabilities & Exploits (CVEs)** page provides a way to identify the security vulnerabilities that impact your devices so you can easily research and address them.

> The **Detected Common Vulnerabilities & Exploits (CVEs)** page is only displayed after a scan is completed and the results for Patch Security are shown. If a scan is stopped before it completes, the **Detected Common Vulnerabilities & Exploits (CVEs)** page is not available.

This page of the Barracuda Security Scanner doesn't provide an additional scan or find additional vulnerabilities. Instead, it organizes the results of the existing scan, specifically the Patch Security results, and expresses them in terms of MITRE Corporation's defined CVEs. Expressing the scan results in terms of CVEs means you can:

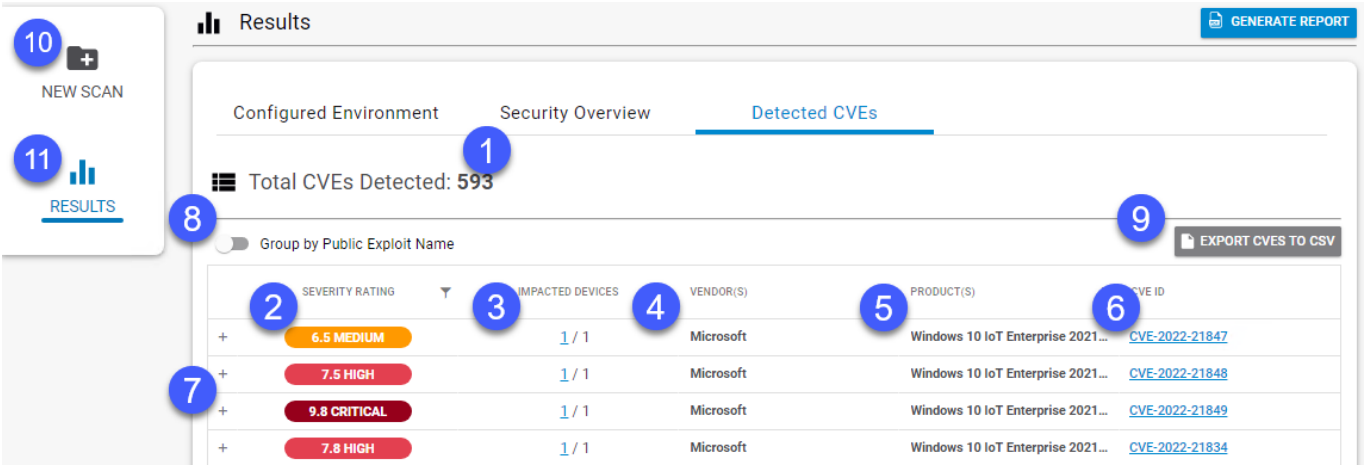
- Identify the existing vulnerabilities
- Assess the severity of each vulnerability
- Easily find mitigation strategies

This page lets you discover more information on:

- Which specific vulnerabilities affect each device
- The severity of the vulnerability
- Which devices are affected
- The affected vendor and product

What are CVEs?

CVEs stands for Common Vulnerabilities and Exposures, which is a program from The MITRE Corporation with the following purpose of identifying, defining, and cataloging publicly disclosed cybersecurity vulnerabilities. CVEs define specific cybersecurity vulnerabilities or exposures and catalog them to streamline the vulnerability disclosure process and to give security professionals common language for discussion.



1. This area displays the total number of CVEs detected on your devices.
2. This icon's color, number, and label indicate the severity of the CVE. The highest severity is 10, the lowest is 0. Possible severities are: **Critical**, **High**, **Medium**, and **Low**. **Reserved** indicates the severity is unknown. **Not Available** indicates the severity is not available. Click the filter icon to sort or filter on these severities.

   About Filters
   When you sort or filter, the table stays filtered, even if you navigate to another tab, until you clear the filters by either:
   - Clicking the filter icon and clicking the **Clear** button.
   - Doing a new scan.
3. The **Impacted Devices** column indicates how many devices are affected, as a fraction of the total assets scanned. Click the link for more details on the impacted devices, including the device names, their Operating Systems, and their IP Addresses.
4. The **Vendor** column displays the name of the software publisher. Click the filter icon to sort or filter on vendor name, including filtering on partial names, excluding names, and other Boolean filtering options.
5. The **Product** column displays the name of the impacted product or products. Click the filter icon to sort or filter on product name, including filtering on partial names, excluding names, and other Boolean filtering options.
6. The **CVE ID** column displays the CVE ID. Click this ID to go to The MITRE Corporation's published report on the CVE.
7. Click the plus icon + next to any row in the table to see a description of the CVE, any potential exploits, and any missing patches that are associated with the CVE.
8. This slider lets you group CVEs by their Public Exploit Name. A public exploit name is the name the exploit is commonly called, as opposed to the official CVE name. For example, CVE-2021-44228 is known to the public as "Log4j". Many CVEs do not have public exploit names. When you group by public exploit name, CVEs without a public exploit name are listed under ***CVEs Without Public Name*** .

   Connection to www.cisa.gov
   When grouping CVEs by Public Exploit name, Barracuda Site Security Scanner connects to www.cisa.gov automatically, and in the background. Occasionally, www.cisa.gov is not

available for certain systems. In this case, the option is unavailable.

9. Click **Export CVEs to CSV** to output a comma separated file of the table that you can open in a spreadsheet application. If the **Group by Public Exploit Name** is On, the CSV is organized by Public Exploit Names.
10. Click **New Scan** to return to the **New Scan/Configuration** page and run another scan.
11. Click **Results** to return to the **Results** page, which displays the scan results organized by categories.

Figures

1. CVEpageArrows.png
2. filter.png
3. filter.png
4. filter.png
5. filter.png
6. Plus_icon.png