



## Vulnerability Dashboard

---

Vulnerability Dashboard enables end users to focus their effort on critical vulnerabilities and workloads that need most attention. You can select relevant scope at the top of this page and select the scoring system for vulnerabilities they want to view (Common Vulnerability Scoring System v2 or v3). The new page highlights the distribution of vulnerabilities in the chosen scope and displays vulnerabilities by different attributes, for example, complexity of exploits, can the vulnerabilities be exploited over the network or does attacker need local access to the workload. Furthermore, there are statistics to quickly filter out vulnerabilities that are remotely exploitable and have lowest complexity to exploit.

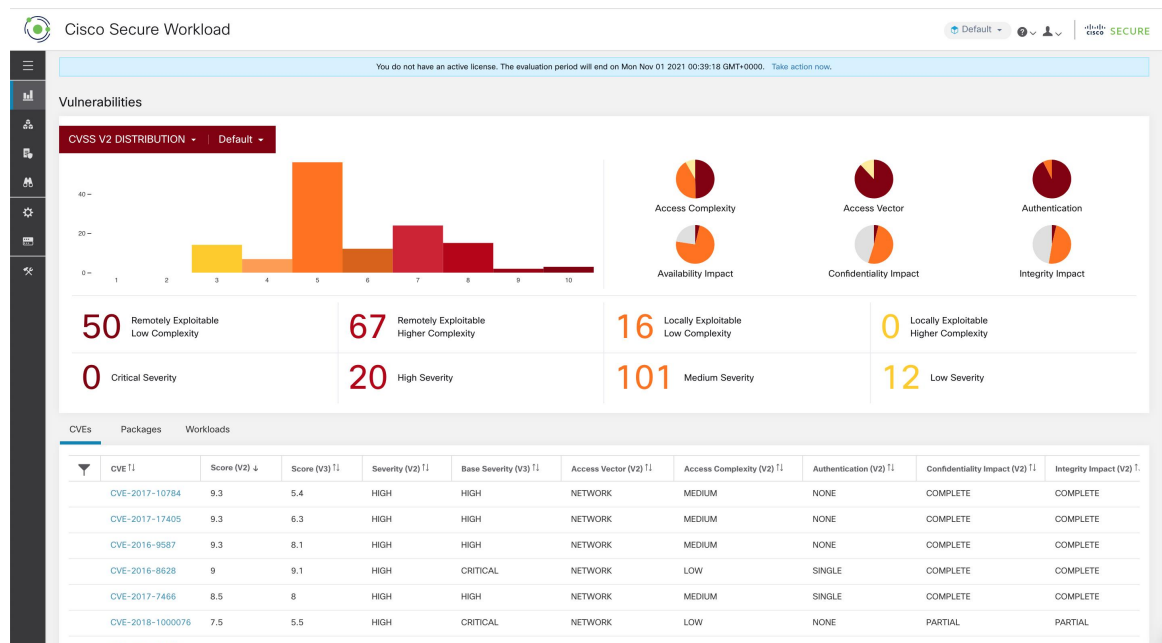
There are three tabs that are available on this page – all of them adjust/filter based on user's clicks on the widgets at the top of the page:

- CVEs tab highlights the vulnerabilities to focus on in the chosen scope.
- Packages tab shows the end users the packages that must be patched.
- Workloads tab lists the workloads that need most attention in terms of patching in the chosen scope.

Clicking on any row in the above tabs display more information about that row, for example, clicking on package row in the packages tab show which workloads that package/version is installed on and the associated vulnerabilities for that package. Similarly, clicking on the row in workloads tab shows packages that are installed on the chosen workload along with the associated vulnerabilities.

This page is intended to help the users identify workloads to focus on first and which packages to patch first.

Figure 1: Vulnerability Dashboard



- [View the Vulnerability Dashboard, on page 2](#)
- [CVEs Tab, on page 2](#)
- [Packages Tab, on page 3](#)
- [Workloads Tab, on page 4](#)

## View the Vulnerability Dashboard

To view the Vulnerability Dashboard, in the left navigation pane, click **Investigate > Vulnerabilities**.

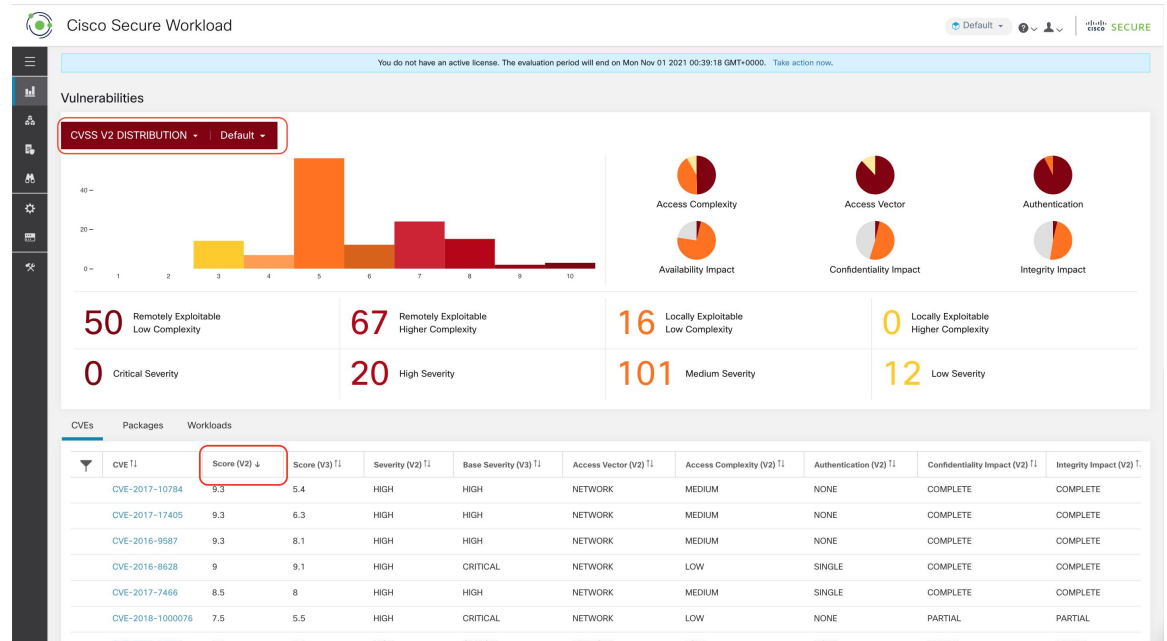
## CVEs Tab

Based on the scope that is selected at the top of the page and the scoring system (v2 or v3), CVE tab highlights the vulnerabilities (sorted by the scores) on workloads in the selected scopes that need attention.

For each CVE, besides basic impact metrics, exploit information based on our threat intelligence is displayed:

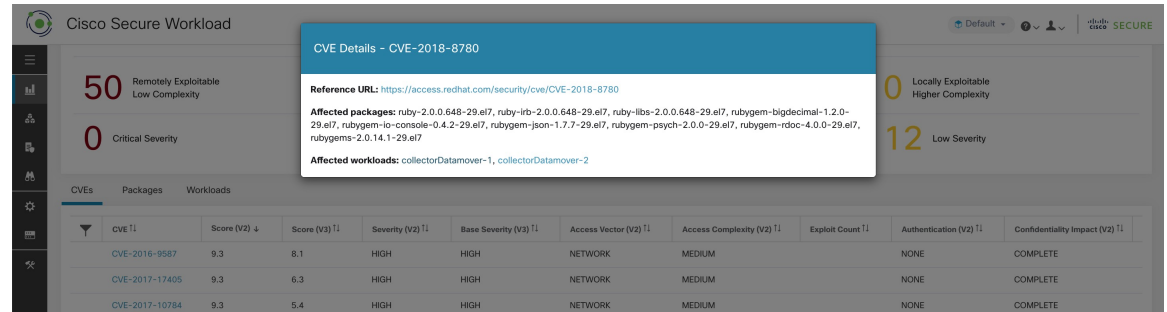
- Exploit Count: number of times CVE was seen exploited in the wild in the last year.
- Last Exploited: last time CVE was seen exploited in the wild by our threat intelligence.

Figure 2: CVEs Tab Listing Vulnerabilities in Specified Scope



Clicking on any row in the CVEs table gives more details about that vulnerability and which workloads that it affects.

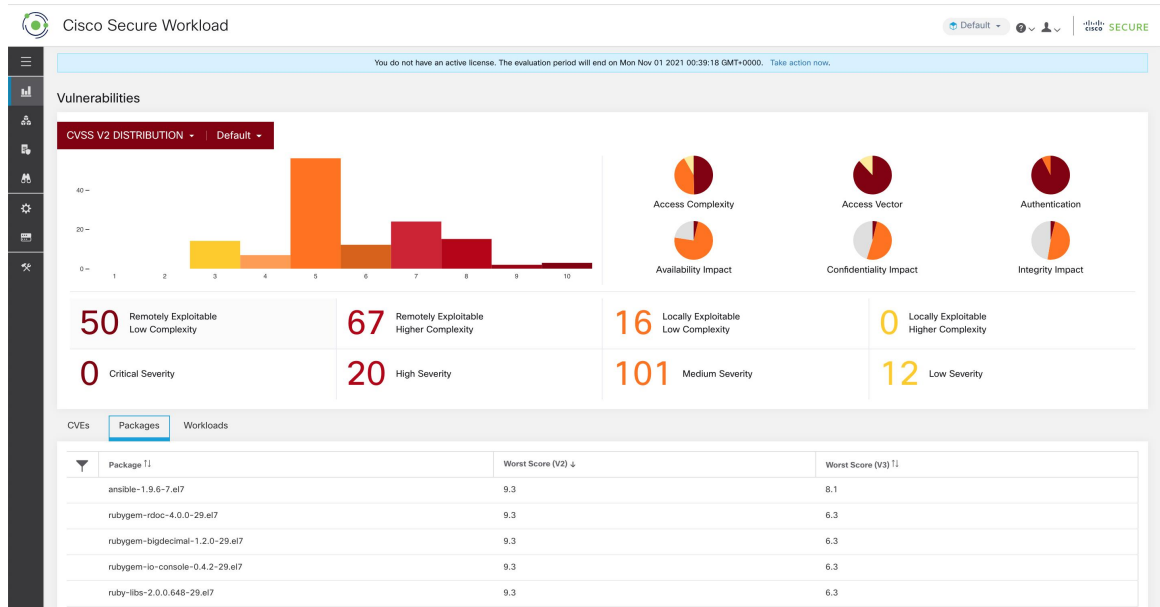
Figure 3: Details for a CVE



## Packages Tab

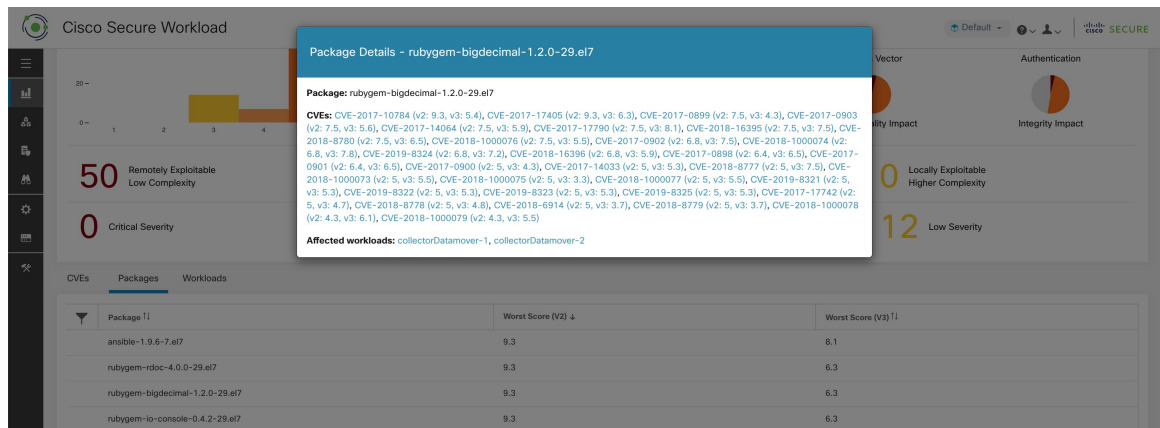
Packages tab lists the software packages that users must pay attention to and potentially upgrade to reduce their attack surface.

Figure 4: Packages Tab Listing Vulnerable Software in Specified Scope



Clicking on any row in the packages table gives more details about which workloads that package is installed as well as the known CVEs for that package.

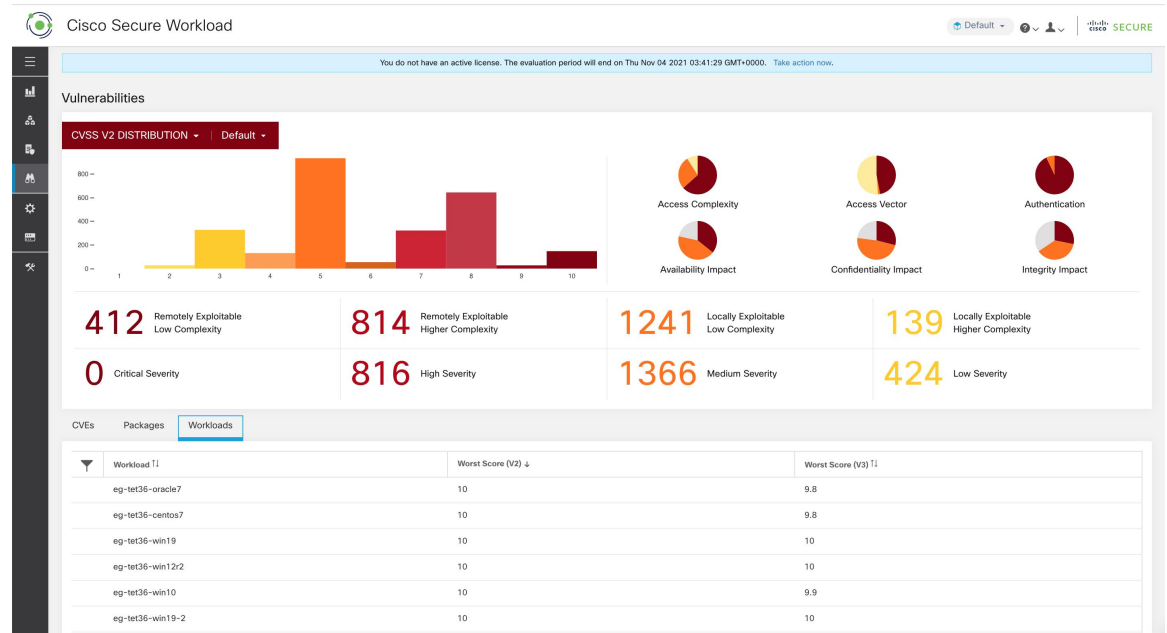
Figure 5: Details of Vulnerabilities and Affected Workloads for a Package



# Workloads Tab

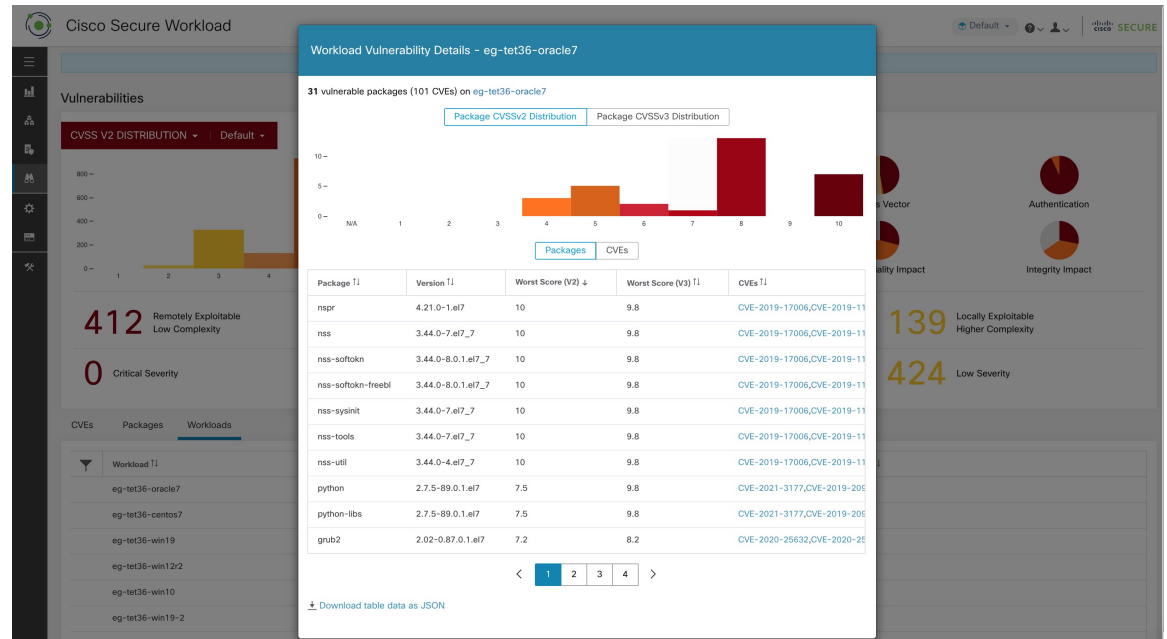
Workloads tab lists the workloads that need attention in terms of software updates or patches.

Figure 6: Workloads Tab Listing Vulnerable Workloads in Specified Scope



Clicking on any row in the workloads table provides the list of packages with vulnerabilities on that workload.

Figure 7: Details of Vulnerabilities for a Workload



All of the above tables are downloadable using the Download links at the bottom of the tables.

