View Vulnerability Dashboard

Cisco Secure Workload identifies and displays a list of the known Common Vulnerabilities and Exposures (CVE) across your workloads on the **Vulnerabilities** page. Using the displayed scores and the severity of the CVEs, you can focus your efforts on the most critical vulnerabilities and workloads that need most attention. Select a scoring system and the scope to view the CVEs according to the severity and other attribute details.

The different scoring systems used in Secure Workload are:

- Common Vulnerability Scoring System (CVSS): CVSS is a qualitative measurement of severity of the CVEs, from low to critical. The scores help you to prioritize responses for the most critical severities. CVSS V3 is the most recent version of the CVSS scoring mechanism.
- Cisco Security Risk Score: The Cisco Security Risk Score provides accurate risk assessments of the CVEs in your workloads. The risk scores help you to comprehend your organization's risk profile and help your security team prioritize remediation strategies.

Table 1: Scoring Systems and Corresponding Attributes

Scoring System	Attributes
Cisco Security Risk Score	• Cisco Security Risk Score with Severity • Active Internet Breach • Easily Exploitable • Fix Available • Malware Exploitable • Popular Target • Predicted Exploitable

Scoring System	Attributes
CVSS V3	• CVE Score with Severity • Attack Complexity • Attack Vector • Availability Impact • Base Severity • Confidentiality Impact • Integrity Impact • Privileges Required • Scope • User Interaction
CVSS V2	• CVE Score with Severity • Access Complexity • Access Vector • Authentication • Availability Impact • Confidentiality Impact • Integrity Impact • Severity

The dashboard 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, the statistics can filter out vulnerabilities that are remotely exploitable and have lowest complexity to exploit.

The CVE threat databases in Secure Workload are updated every 24 hours by retrieving the latest CVE details from popular sources such as NIST, Microsoft, Oracle, and Cisco Vulnerability Management. If the Secure Workload cluster is in an air-gapped environment, the CVE threat data packs must be downloaded from https://updates.tetrationcloud.com and uploaded in Secure Workload.

The CVE threat databases in Secure Workload are updated every 24 hours by retrieving the latest CVE details from popular sources such as NIST, Microsoft, and Oracle. If the Secure Workload cluster is in an air-gapped environment, the CVE threat data packs must be downloaded from https://updates.tetrationcloud.com and uploaded in Secure Workload.

By using the scores and the required attributes of the known CVEs in your workloads, you can:

- Create inventory filters. See Inventory Filters.
- Configure microsegmentation policies to block the external communication from the impacted workloads and publish virtual patching rules to Cisco Secure Firewall Management Center.

Table 2: Feature Information

Feature Name	Release	Feature Description	Where to Find
Integration of Cisco Vulnerability Management for Deep CVE Insights with Cisco Risk Score for Prioritization	3.9 Patch 2	You can use the Cisco Security Risk Scores of the CVEs to create inventory filters, microsegmentation policies to block communication from the impacted workloads, and virtual patching rules to publish the CVEs to Cisco Secure Firewall.	Vulnerability Dashboard, on page 3 Cisco Security Risk Score-Based Filter

Vulnerability Dashboard

To view the Vulnerabilities page, from the navigation pane, choose **Investigate** > **Vulnerabilities**. The vulnerabilities identified using the different scoring system are displayed. The graphs and widgets display the number of vulnerabilities with the associated risk level and attributes depending on the scoring systemts to identify workloads which requires immediate attention and the packages which needs to be patched immediately to reduce the risks.

Figure 1: Vulnerabilities Page

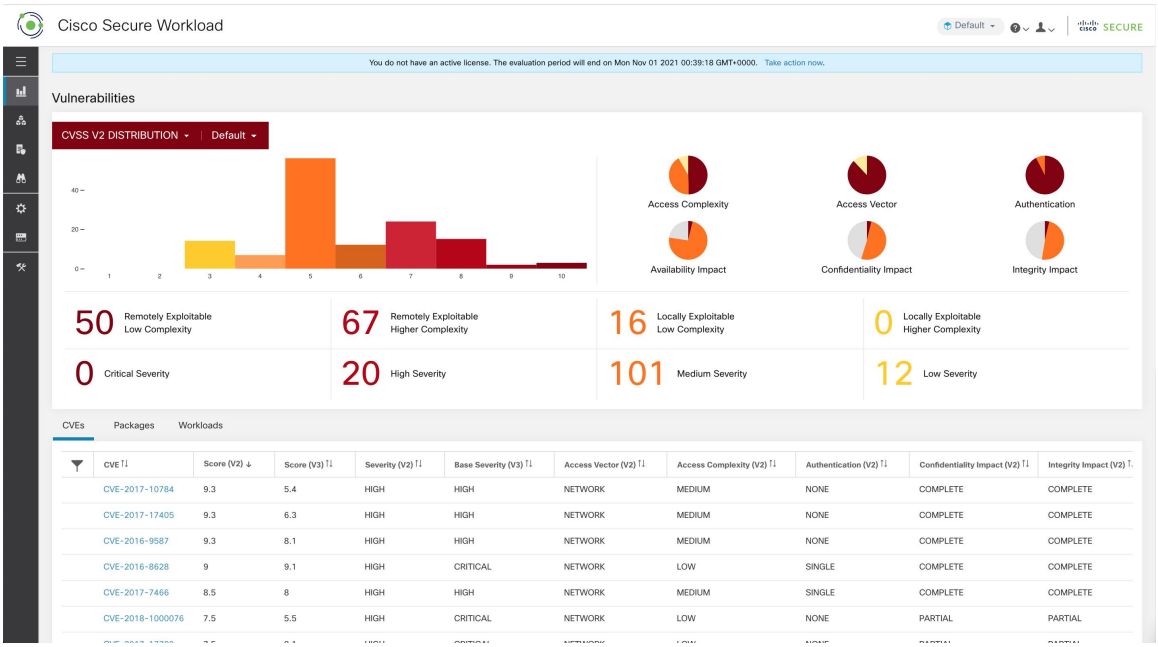
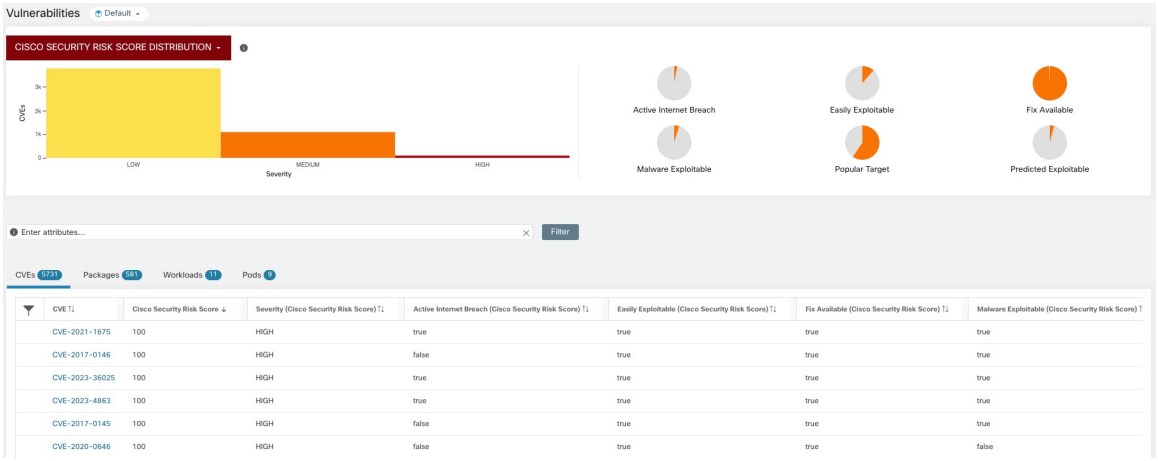


Figure 2: Vulnerabilities Page



The following tabs are filtered based on the selected portion of the graphs or widgets:

- The **CVEs** tab highlight the vulnerabilities that requires attention in the selected scope.
- The **Packages** tab lists the packages that must be patched.
- The **Workloads** tab lists the impacted workloads in the selected scope.
- The **Pods** tabs lists the impacted Kubernetes pods in the selected scope.

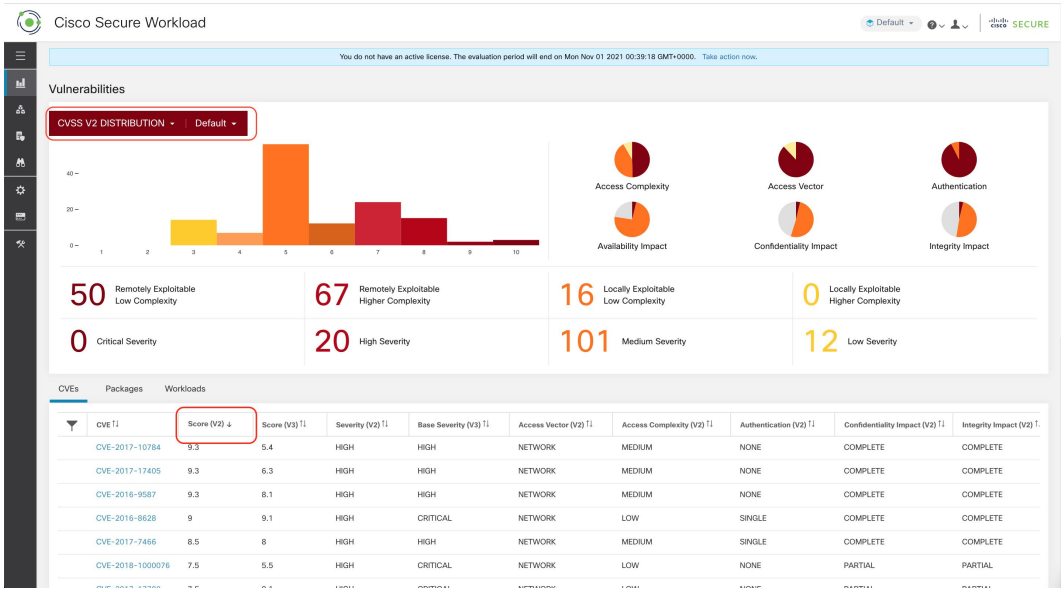
For details, click the required row in the tabs. For example, click a row in the Packages tab to view the workloads where the package or version is installed and the associated vulnerabilities for the package. The displayed lists can be downloaded as a JSON or CSV file using the download links.

CVEs Tab

Based on the scoring system and selected scope, the CVEs tab lists the vulnerabilities identified on the workloads. For each CVE, besides basic impact metrics, exploit information based on Secure Workload's threat intelligence is displayed:

- Exploit Count: Number of times the CVE was seen exploited in the organizations in the previous year.
- Last Exploited: Last time the CVE was seen exploited in the organizations by Secure Workload's threat intelligence.

Figure 3: CVEs Tab Listing Vulnerabilities in Specified Scope



The graphs and pie chart can be used to filter the CVEs based on the severity or the required attributes of the scoring system. For example, if you click the Critical severity bar in any of the scoring system, the table will display only the workloads, packages, and pods containing the critical CVEs.

Click the requied row under the CVEs tab to get more details on that vulnerability and the impacted workloads.

Figure 4: Details for a CVE

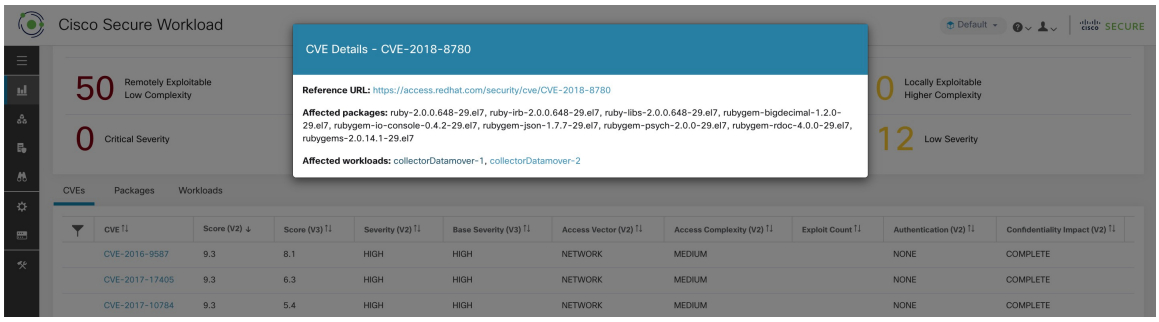
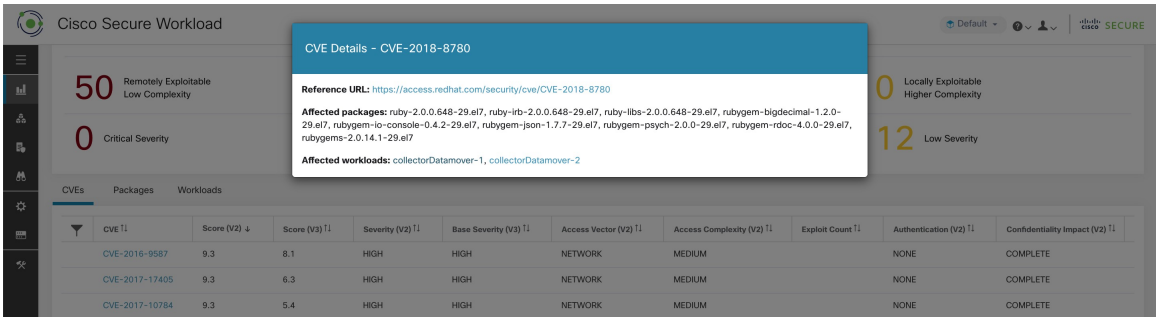


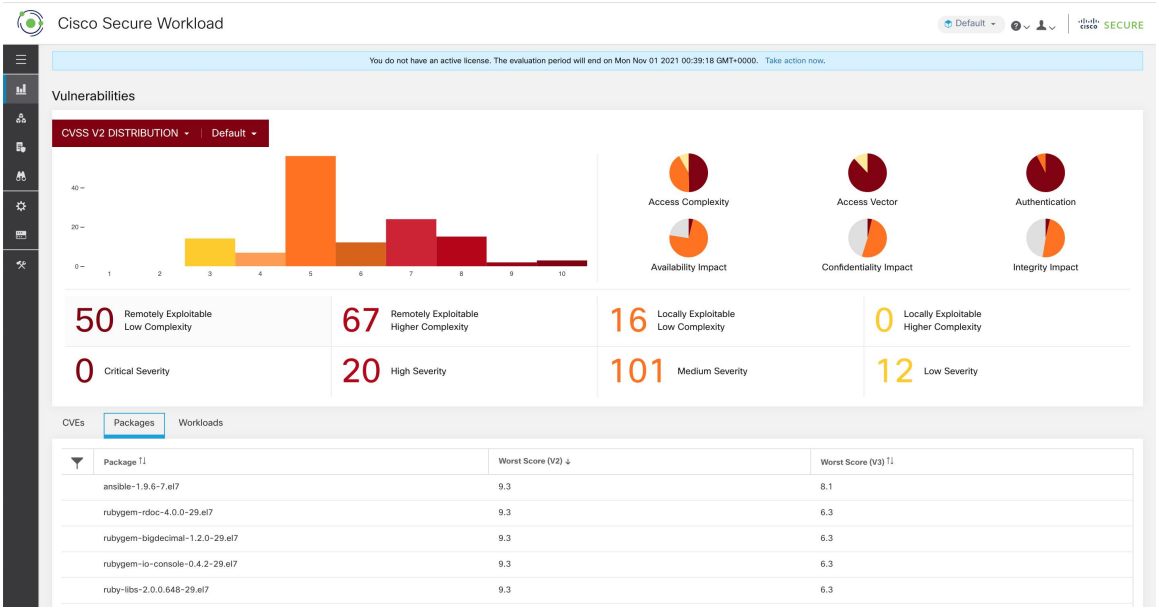
Figure 5: Details for a CVE



Packages Tab

The Packages tab lists the imapcted software packages that must be upgraded to reduce their attack surface.

Figure 6: Packages Tab Listing Vulnerable Software in Specified Scope



Click the requied row under the Packages tab to get more details on impacted packages, the workloads with the packages, and the identified CVEs in the packages.

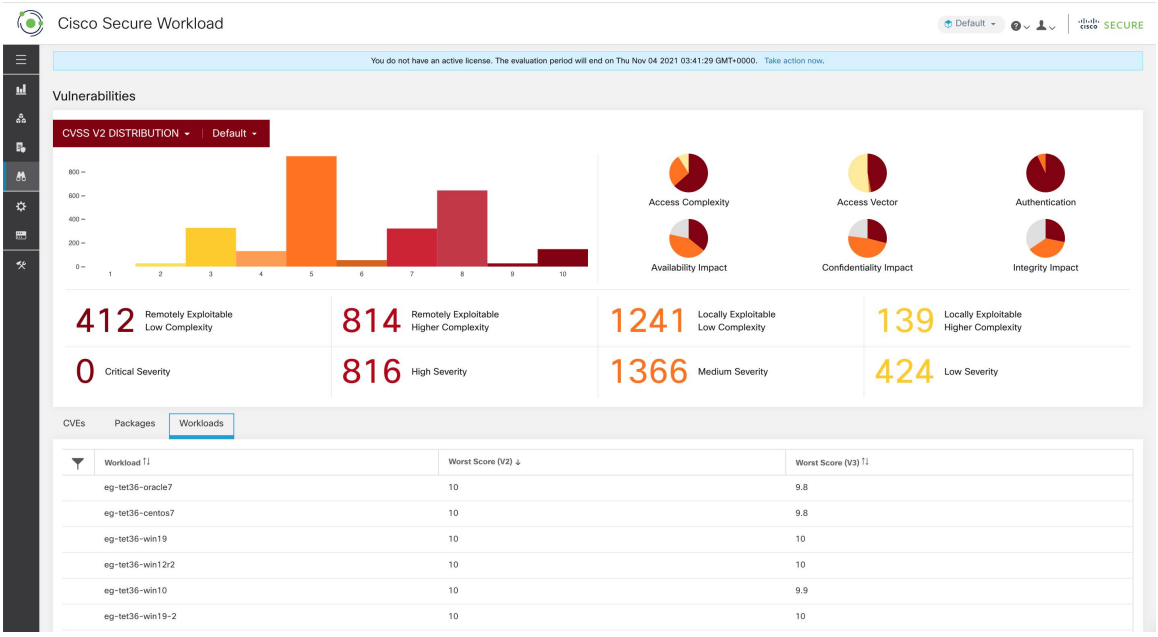
Figure 7: Details of Vulnerabilities and Affected Workloads for a Package

Figure 8: Details of Vulnerabilities and Affected Workloads for a Package

Workloads Tab

The Workloads tab lists the workloads that require immediate attention in terms of software updates or patches.

Figure 9: Workloads Tab Listing Vulnerable Workloads in Specified Scope



Click the requied row under the Workloads tab to get more details on vulnerable packages present in the selected workload. To view the workload profile, click the workload name next to the title of the dialog box.

Figure 10: Vulnerabilities Details in an Impacted Workload

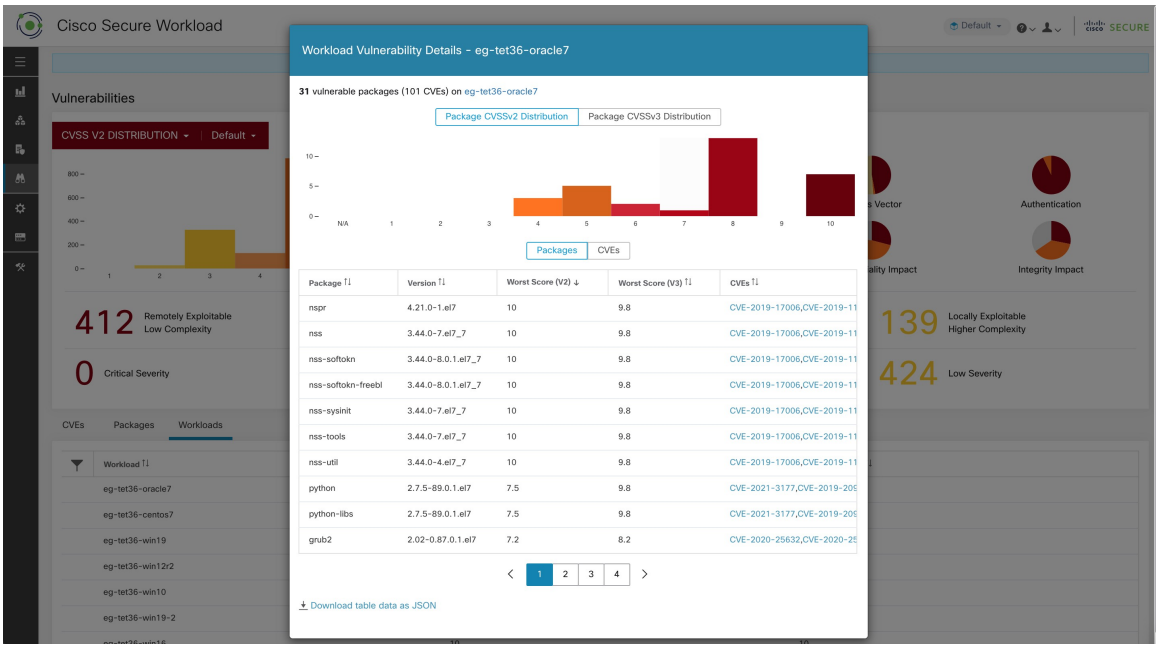
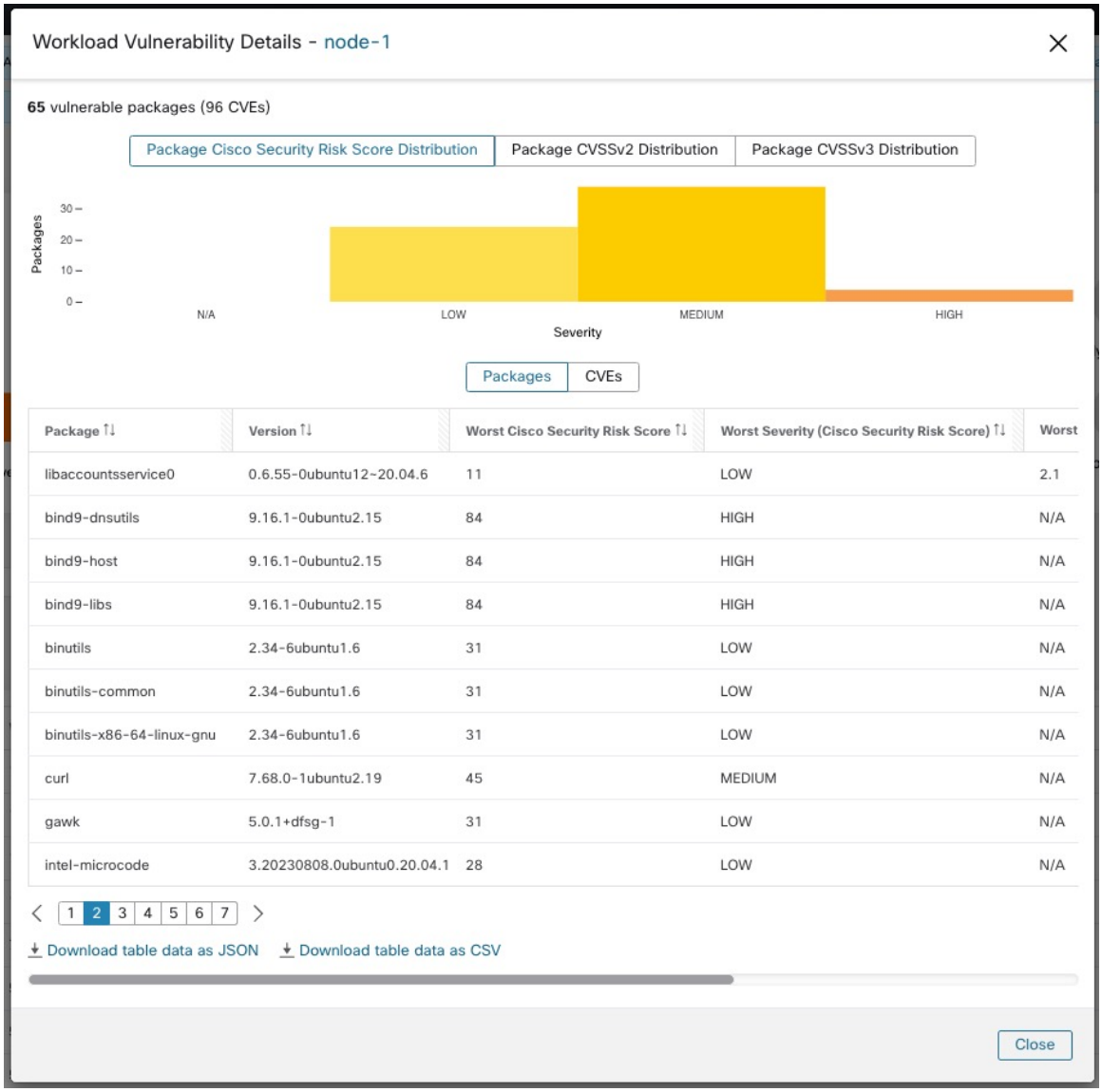


Figure 11: Vulnerabilities Details in an Impacted Workload



Pods Tab

The Pods tab lists the Kubernetes pods that require immediate attention in terms of software updates or patches.

Click the requied row under the Pods tab to get more details on impacted Kubernetes pod, packages, images, and the identified CVEs.

Figure 12: CVEs and Affected Packages in a Kubernetes Pod