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.

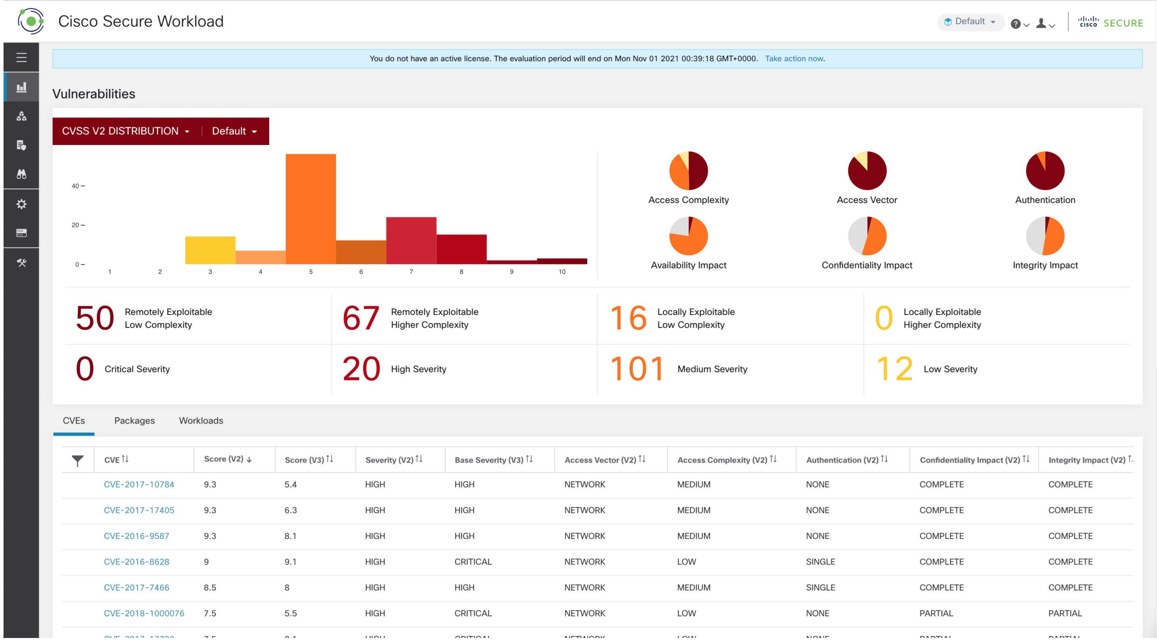
There are three tabs that are available on this page – all of them adjust/filter based on user’s clicks on the widgets at the top of the page:

- 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



You do not have an active license. The evaluation period will end on Mon Nov 01 2021 00:39:18 GMT+0000. Take action now.

Vulnerabilities

50 Remotely Exploitable Low Complexity

67 Remotely Exploitable Higher Complexity

16 Locally Exploitable Low Complexity

0 Locally Exploitable Higher Complexity

0 Critical Severity

20 High Severity

101 Medium Severity

12 Low Severity

CVE	Score (V2)	Score (V3)	Severity (V2)	Base Severity (V3)	Access Vector (V2)	Access Complexity (V2)	Authentication (V2)	Confidentiality Impact (V2)	Integrity Impact (V2)
CVE-2017-10784	9.3	5.4	HIGH	HIGH	NETWORK	MEDIUM	NONE	COMPLETE	COMPLETE
CVE-2017-17405	9.3	6.3	HIGH	HIGH	NETWORK	MEDIUM	NONE	COMPLETE	COMPLETE
CVE-2016-9587	9.3	8.1	HIGH	HIGH	NETWORK	MEDIUM	NONE	COMPLETE	COMPLETE
CVE-2016-8628	9	9.1	HIGH	CRITICAL	NETWORK	LOW	SINGLE	COMPLETE	COMPLETE
CVE-2017-7466	8.5	8	HIGH	HIGH	NETWORK	MEDIUM	SINGLE	COMPLETE	COMPLETE
CVE-2018-1000076	7.5	5.5	HIGH	CRITICAL	NETWORK	LOW	NONE	PARTIAL	PARTIAL

View the Vulnerability Dashboard

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

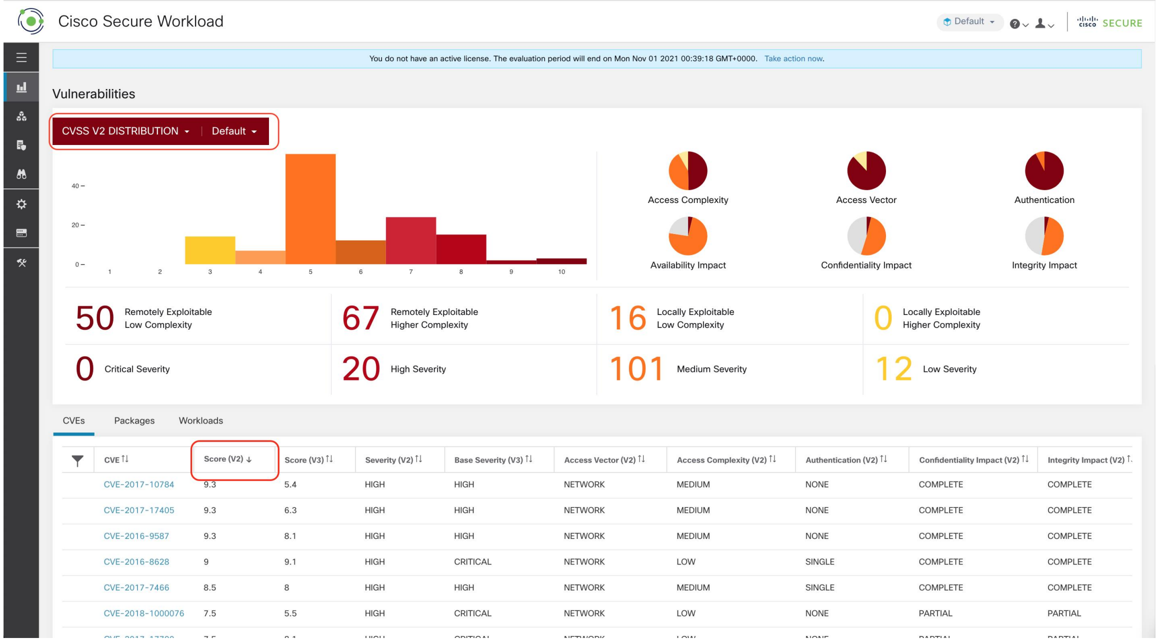
CVEs Tab

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



You do not have an active license. The evaluation period will end on Mon Nov 01 2021 00:39:18 GMT+0000. Take action now.

50 Remotely Exploitable Low Complexity

67 Remotely Exploitable Higher Complexity

16 Locally Exploitable Low Complexity

0 Locally Exploitable Higher Complexity

0 Critical Severity

20 High Severity

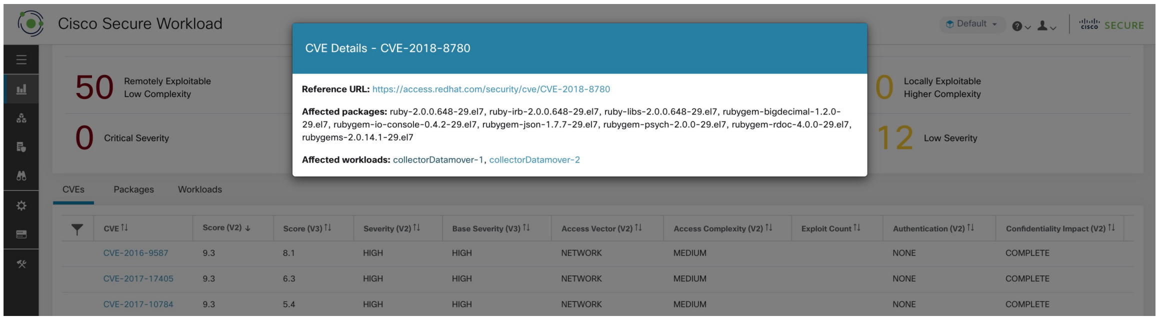
101 Medium Severity

12 Low Severity

CVE ⇅	Score (V2) ↓	Score (V3) ⇅	Severity (V2) ⇅	Base Severity (V3) ⇅	Access Vector (V2) ⇅	Access Complexity (V2) ⇅	Authentication (V2) ⇅	Confidentiality Impact (V2) ⇅	Integrity Impact (V2) ⇅
CVE-2017-10784	9.3	5.4	HIGH	HIGH	NETWORK	MEDIUM	NONE	COMPLETE	COMPLETE
CVE-2017-17405	9.3	6.3	HIGH	HIGH	NETWORK	MEDIUM	NONE	COMPLETE	COMPLETE
CVE-2016-9587	9.3	8.1	HIGH	HIGH	NETWORK	MEDIUM	NONE	COMPLETE	COMPLETE
CVE-2016-8628	9	9.1	HIGH	CRITICAL	NETWORK	LOW	SINGLE	COMPLETE	COMPLETE
CVE-2017-7466	8.5	8	HIGH	HIGH	NETWORK	MEDIUM	SINGLE	COMPLETE	COMPLETE
CVE-2018-1000076	7.5	5.5	HIGH	CRITICAL	NETWORK	LOW	NONE	PARTIAL	PARTIAL

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



50 Remotely Exploitable Low Complexity

0 Critical Severity

0 Locally Exploitable Higher Complexity

12 Low Severity

CVE Details - CVE-2018-8780

Reference URL: https://access.redhat.com/security/cve/CVE-2018-8780

Affected packages: ruby-2.0.0.648-29.el7, ruby-irb-2.0.0.648-29.el7, ruby-libs-2.0.0.648-29.el7, rubygem-bigdecimal-1.2.0-29.el7, rubygem-io-console-0.4.2-29.el7, rubygem-json-1.7.7-29.el7, rubygem-psych-2.0.0-29.el7, rubygem-rdoc-4.0.0-29.el7, rubygems-2.0.14.1-29.el7

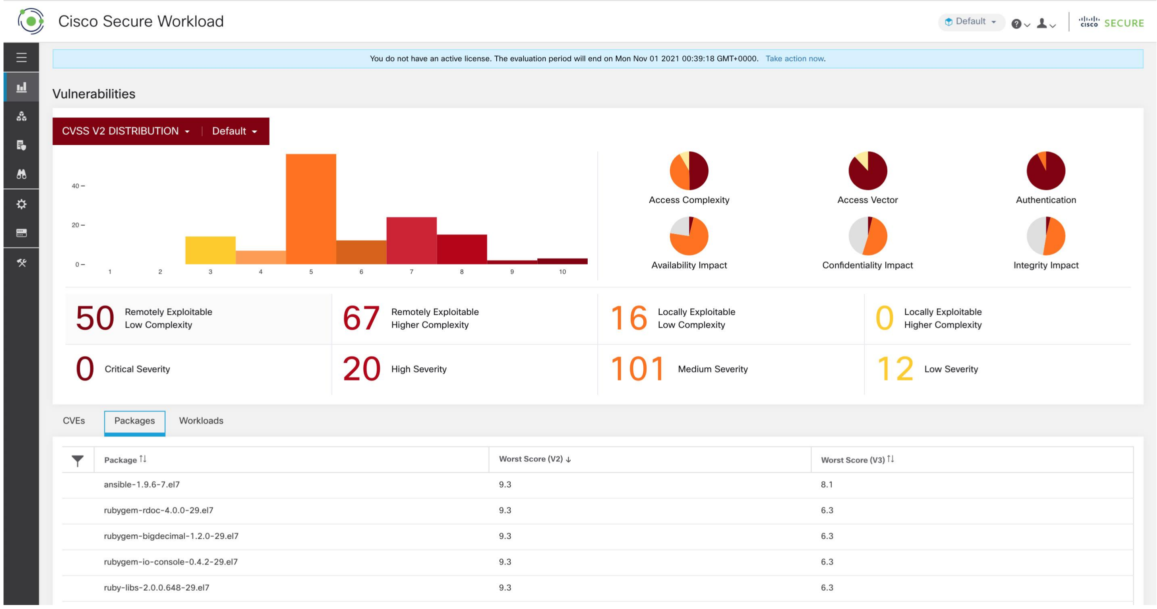
Affected workloads: collectorDatamover-1, collectorDatamover-2

CVE ⇅	Score (V2) ↓	Score (V3) ⇅	Severity (V2) ⇅	Base Severity (V3) ⇅	Access Vector (V2) ⇅	Access Complexity (V2) ⇅	Exploit Count ⇅	Authentication (V2) ⇅	Confidentiality Impact (V2) ⇅
CVE-2016-9587	9.3	8.1	HIGH	HIGH	NETWORK	MEDIUM		NONE	COMPLETE
CVE-2017-17405	9.3	6.3	HIGH	HIGH	NETWORK	MEDIUM		NONE	COMPLETE
CVE-2017-10784	9.3	5.4	HIGH	HIGH	NETWORK	MEDIUM		NONE	COMPLETE

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

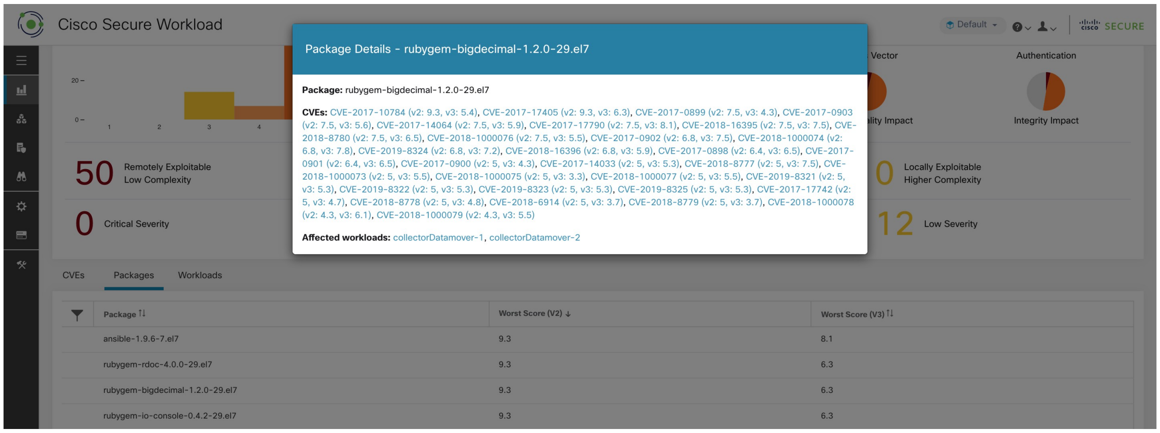


You do not have an active license. The evaluation period will end on Mon Nov 01 2021 00:39:18 GMT+0000. Take action now.

Package ↑↓	Worst Score (V2) ↓	Worst Score (V3) ↑↓
ansible-1.9.6-7.el7	9.3	8.1
rubygem-rdoc-4.0.0-29.el7	9.3	6.3
rubygem-bigdecimal-1.2.0-29.el7	9.3	6.3
rubygem-io-console-0.4.2-29.el7	9.3	6.3
ruby-libs-2.0.0.648-29.el7	9.3	6.3

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



Package Details - rubygem-bigdecimal-1.2.0-29.el7

Package: rubygem-bigdecimal-1.2.0-29.el7

CVEs: CVE-2017-10784 (v2: 9.3, v3: 5.4), CVE-2017-17405 (v2: 9.3, v3: 6.3), CVE-2017-0899 (v2: 7.5, v3: 4.3), CVE-2017-0903 (v2: 7.5, v3: 5.6), CVE-2017-14064 (v2: 7.5, v3: 5.9), CVE-2017-17790 (v2: 7.5, v3: 8.1), CVE-2018-16395 (v2: 7.5, v3: 7.5), CVE-2018-8780 (v2: 7.5, v3: 6.5), CVE-2018-1000076 (v2: 7.5, v3: 5.5), CVE-2017-0902 (v2: 6.8, v3: 7.5), CVE-2018-1000074 (v2: 6.8, v3: 7.8), CVE-2019-8324 (v2: 6.8, v3: 7.2), CVE-2018-16396 (v2: 6.8, v3: 5.9), CVE-2017-0898 (v2: 6.4, v3: 6.5), CVE-2017-0901 (v2: 6.4, v3: 6.5), CVE-2017-0900 (v2: 5, v3: 4.3), CVE-2017-14033 (v2: 5, v3: 5.3), CVE-2018-8777 (v2: 5, v3: 7.5), CVE-2018-1000073 (v2: 5, v3: 5.5), CVE-2018-1000075 (v2: 5, v3: 3.3), CVE-2018-1000077 (v2: 5, v3: 5.5), CVE-2019-8321 (v2: 5, v3: 5.3), CVE-2019-8322 (v2: 5, v3: 5.3), CVE-2019-8323 (v2: 5, v3: 5.3), CVE-2019-8325 (v2: 5, v3: 5.3), CVE-2017-17742 (v2: 5, v3: 4.7), CVE-2018-8778 (v2: 5, v3: 4.8), CVE-2018-6914 (v2: 5, v3: 3.7), CVE-2018-8779 (v2: 5, v3: 3.7), CVE-2018-1000078 (v2: 4.3, v3: 6.1), CVE-2018-1000079 (v2: 4.3, v3: 5.5)

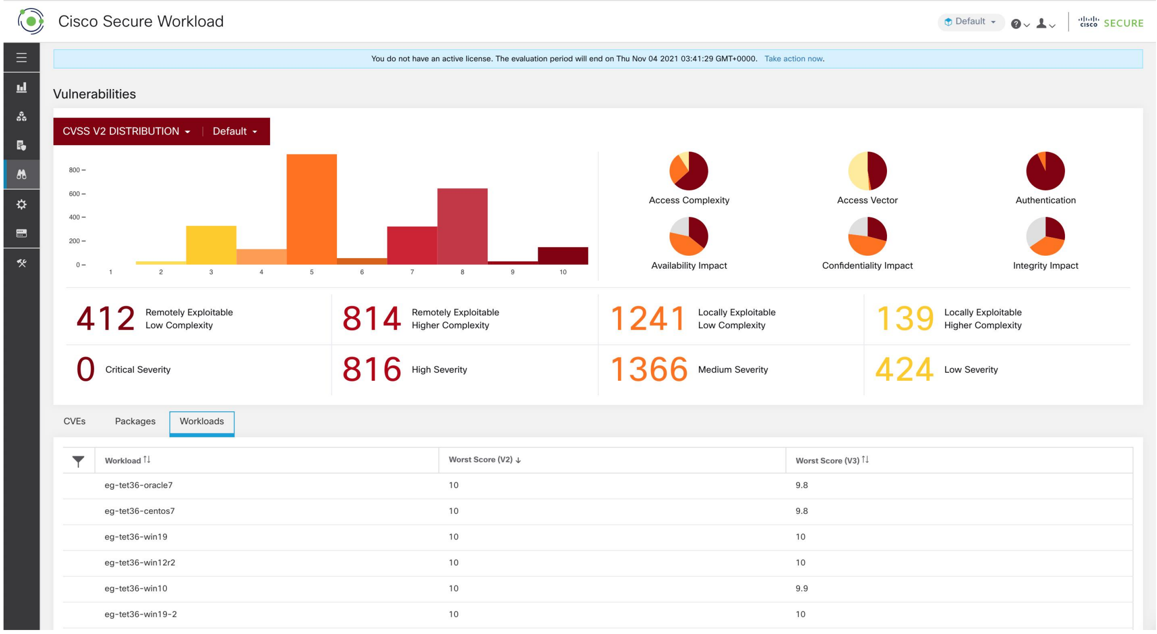
Affected workloads: collectorDatamover-1, collectorDatamover-2

Package ↑↓	Worst Score (V2) ↓	Worst Score (V3) ↑↓
ansible-1.9.6-7.el7	9.3	8.1
rubygem-rdoc-4.0.0-29.el7	9.3	6.3
rubygem-bigdecimal-1.2.0-29.el7	9.3	6.3
rubygem-io-console-0.4.2-29.el7	9.3	6.3

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



You do not have an active license. The evaluation period will end on Thu Nov 04 2021 03:41:29 GMT+0000. Take action now.

Vulnerabilities

412 Remotely Exploitable Low Complexity

814 Remotely Exploitable Higher Complexity

1241 Locally Exploitable Low Complexity

139 Locally Exploitable Higher Complexity

0 Critical Severity

816 High Severity

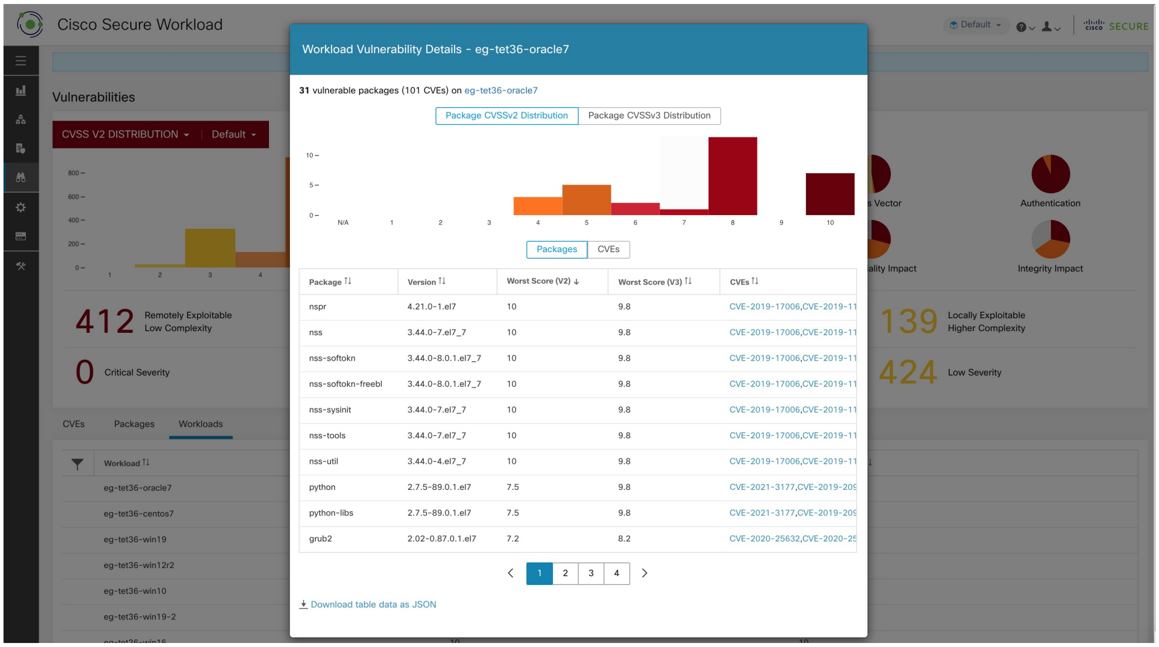
1366 Medium Severity

424 Low Severity

Workload ⇅	Worst Score (V2) ↓	Worst Score (V3) ⇅
eg-tet36-oracle7	10	9.8
eg-tet36-centos7	10	9.8
eg-tet36-win19	10	10
eg-tet36-win12r2	10	10
eg-tet36-win10	10	9.9
eg-tet36-win19-2	10	10

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



Workload Vulnerability Details - eg-tet36-oracle7

31 vulnerable packages (101 CVEs) on eg-tet36-oracle7

Package ⇅	Version ⇅	Worst Score (V2) ↓	Worst Score (V3) ⇅	CVEs ⇅
nspr	4.21.0-1.el7	10	9.8	CVE-2019-17006,CVE-2019-11
nss	3.44.0-7.el7_7	10	9.8	CVE-2019-17006,CVE-2019-11
nss-softokn	3.44.0-8.0.1.el7_7	10	9.8	CVE-2019-17006,CVE-2019-11
nss-softokn-freebl	3.44.0-8.0.1.el7_7	10	9.8	CVE-2019-17006,CVE-2019-11
nss-sysinit	3.44.0-7.el7_7	10	9.8	CVE-2019-17006,CVE-2019-11
nss-tools	3.44.0-7.el7_7	10	9.8	CVE-2019-17006,CVE-2019-11
nss-util	3.44.0-4.el7_7	10	9.8	CVE-2019-17006,CVE-2019-11
python	2.7.5-89.0.1.el7	7.5	9.8	CVE-2021-3177,CVE-2019-20
python-libs	2.7.5-89.0.1.el7	7.5	9.8	CVE-2021-3177,CVE-2019-20
grub2	2.02-0.87.0.1.el7	7.2	8.2	CVE-2020-25632,CVE-2020-25

‹ 1 2 3 4 ›

Download table data as JSON

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