

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.

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.

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		

Table 2: Feature Information

- Vulnerability Dashboard, on page 3
- CVEs Tab, on page 5
- Packages Tab, on page 6
- Workloads Tab, on page 7
- Pods Tab, on page 9

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

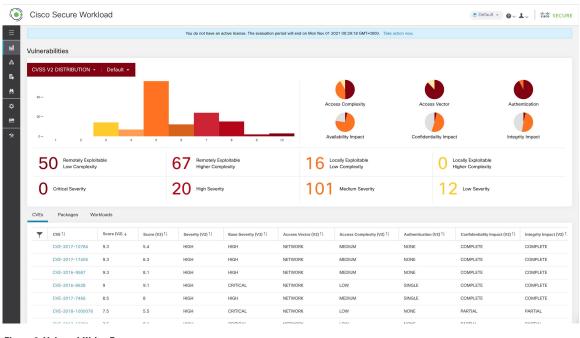
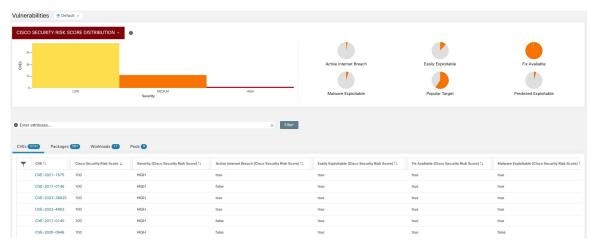


Figure 2: Vulnerabilities Page



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.

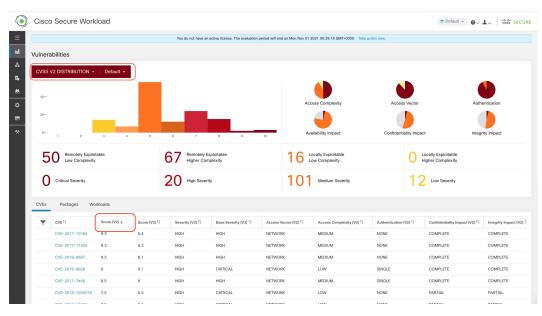


Figure 3: CVEs Tab Listing Vulnerabilities in Specified Scope

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

	co Secure Worl	kload	CVE Det	ails - CVE-2018-	·8780				Default	● ●~ ▲~ diada SEC
ب (Critical Severity		Affected pa 29.el7, ruby rubygems-2	Reference URL: https://access.redhat.com/security/cve/CVE-2018-8760 Affected packages: ruby-2.0.0.648-29.al7, ruby-ib-2.0.0.648-29.al7, ruby-ibs-2.0.0.648-29.al7, rubygem-bigdecimal-1.2.0- 29.al7, rubygem-io-console-0.42-29.al7, rubygem-json-1.7.7-29.al7, rubygem-psych-2.0.0-29.al7, rubygem-rdoc-4.0.0-29.al7, rubygems-2.0.1.1-29.al7 Affected workloads: collector/Datamover-1, collector/Datamover-2					0 Locally Exploitable Higher Complexity 12 Low Seventy	
CVEs	s Packages W	orkloads								
CVEs	Packages W	forkloads Score (V2) ↓	Score (V3) 1	Severity (V2) 1	Base Severity (V3) 🗍	Access Vector (V2)	Access Complexity (V2)	Exploit Count 14	Authentication (V2)	Confidentiality Impact (V2) 1
CVEs	_		Score (V3) 11 8.1	Severity (V2) 11 HIGH	Base Severity (V3) ^{TL} HIGH	Access Vector (V2)	Access Complexity (V2) 11 MEDIUM	Exploit Count 1	Authentication (V2)	Confidentiality Impact (V2)
CVEs	CVE 1	Score (V2) ↓						Exploit Count 1		

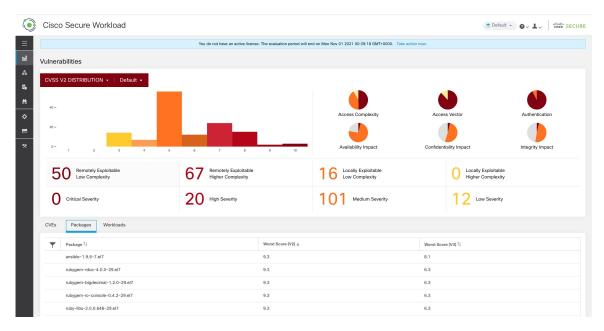
Figure 5: Details for a CVE

Cisco Secure Workload			OVE Do	tails - CVE-2018	- 9790				Default	● ●~ ↓~ "duth secu	
5	50 Remotely Exploitable Low Complexity			Reference URL: https://access.redhat.com/security/cve/CVE-2018-8780 Affected packages: ndy-2.0.648-29.el7, ndy-itb-2.0.648-29.el7, ndy-itb-2.0.648-29.el7, ndy-gen-bigdecimal-1.2.0-							
C	Critical Severity		rubygems-	29.af7, tubygem-lo-console-0.4.2-29.ef7, rubygem-json-1.7.7-28.ef7, rubygem-psych-2.0.0-29.ef7, rubygem-rdoc-4.0.0-29.ef7 rubygems-2.0.14.1-29.ef7 Affected workloads: collector/Datamover-1, collector/Datamover-2					12 Low Severity		
CVEs	-	orkloads									
T	CVE 11	Score (V2) ↓	Score (V3) ^{†↓}	Severity (V2) ^{↑↓}	Base Severity (V3) ^{†↓}	Access Vector (V2)	Access Complexity (V2)	Exploit Count 1	Authentication (V2)	Confidentiality Impact (V2)	
_	CVE-2016-9587	Score (V2) ↓ 9.3	Score (V3) 11 8.1	Severity (V2)	Base Severity (V3) TI HIGH	Access Vector (V2) 11 NETWORK	Access Complexity (V2)	Exploit Count 1	Authentication (V2)	Confidentiality Impact (V2)	
_								Exploit Count 11			

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

٢	Cisco Secure Workload			Default	• Ø~ L.
≡		Package Details - rubygem-bigd	ecimal-1.2.0-29.el7	Vector	Authentication
ы	20 -	Package: rubygem-bigdecimal-1.2.0-29.e	17		
80	0- 1 2 3 ·	4 (v2: 7.5, v3: 5.6), CVE-2017-14064 (v2: 7.	CVE-2017-17405 (v2: 9.3, v3: 6.3), CVE-2017-0899 (v2: 7.5, v3: 4.3), CV 5, v3: 5.9), CVE-2017-17790 (v2: 7.5, v3: 8.1), CVE-2018-16395 (v2: 7.5, 000076 (v2: 7.5, v3: 5.5), CVE-2017-0902 (v2: 6.8, v3: 7.5), CVE-2018-10	v3: 7.5), CVE- lity Impact	Integrity Impact
68	50 Remotely Exploitable Low Complexity	6.8, v3: 7.8), CVE-2019-8324 (v2: 6.8, v3: 0901 (v2: 6.4, v3: 6.5), CVE-2017-0900 (v 2018-1000073 (v2: 5, v3: 5.5), CVE-2018-	00007b (W2: 7.5, V3: 5.5), CVE-2017-9002 (V2: 5.8, V3: 7.5), CVE-2018-1 22, CVE-2018-10396 (V2: 6.3 V3: 5.9), CVE-2017-0898 (V2: 6.4, V3: 6.1 22; 5, V3: 4.3), CVE-2017-14033 (V2: 5, V3: 5.3), CVE-2018-8777 (V2: 5, V3: 1000075 (V2: 5, V3: 3.3), CVE-2018-1000077 (V2: 5, V3: 5.5), CVE-2019- VE-2019-8232 (V2: 5, V3: 5.3), CVE-2018-1000077 (V2: 5, V3: 5.5), CVE-2019- VE-2019-8232 (V2: 5, V3: 5.3), CVE-2018-100077 (V2: 5, V3: 5.5), CVE-2019- VE-2019-8232 (V2: 5, V3: 5.3), CVE-2018-100077 (V2: 5, V3: 5.5), CVE-2019- VE-2019-8232 (V2: 5, V3: 5.3), CVE-2018-100077 (V2: 5, V3: 5.5), CVE-2019- VE-2019-8232 (V2: 5, V2: 5,	5), CVE-2017- 3: 7.5), CVE- 8321 (v2: 5, Higher Complexity	
¢ 	O Critical Severity	5, v3: 4.7), CVE-2018-8778 (v2: 5, v3: 4.8) (v2: 4.3, v3: 6.1), CVE-2018-1000079 (v2: Affected workloads: collectorDatamover-1		12 Low Severity	
*	CVEs Packages Workloads			_	
	Package 1		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	

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

Package Details - firefox102.15.0-1.el7.centos	<
Package: firefox102.15.0-1.el7.centos	
CVEs: CVE-2023-4051 (v2: N/A, v3: 7.5, Cisco Security Risk Score: 50.1), CVE-2023-4053 (v2: N/A, v3: 6.1, Cisc Security Risk Score: 50.1), CVE-2023-4573 (v2: N/A, v3: 7.5, Cisco Security Risk Score: 50.1), CVE-2023-4574 (vN/A, v3: 7.5, Cisco Security Risk Score: 50.1), CVE-2023-4575 (v2: N/A, v3: 7.5, Cisco Security Risk Score: 50.1), CVE-2023-4577 (v2: N/A, v3: 7.5, Cisco Security Risk Score: 50.1), CVE-2023-4577 (v2: N/A, v3: 7.5, Cisco Security Risk Score: 50.1), CVE-2023-4577 (v2: N/A, v3: 7.5, Cisco Security Risk Score: 50.1), CVE-2023-4578 (v2: N/A, v3: 6.1, Cisco Security Risk Score: 50.1), CVE-2023-4580 (v2: N/A, v3: 6.1, Cisco Security Risk Score: 50.1), CVE-2023-4580 (v2: N/A, v3: 6.1, Cisco Security Risk Score: 50.1), CVE-2023-4583 (v2: N/A, v3: 7.5, Cisco Security Risk Score: 50.1), CVE-2023-4583 (v2: N/A, v3: 7.5, Cisco Security Risk Score: 50.1), CVE-2023-4584 (v2: N/A, v3: 8.8, Cisco Security Risk Score: 55.7), CVE-2023-4584 (v2: N/A, v3: 8.8, Cisco Security Risk Score: 55.7), CVE-2023-3600 (v2: N/A, v3: 8.8, Cisco Security Risk Score: 55.7), CVE-2023-5169 (vN/A, v3: 6.5, Cisco Security Risk Score: 50.2), CVE-2023-5171 (v2: N/A, v3: 6.5, Cisco Security Risk Score: 50.2), CVE-2023-5171 (v2: N/A, v3: 6.5, Cisco Security Risk Score: 50.2), CVE-2023-5176 (v2: N/A, v3: 9.8, Cisco Security Risk Score: 55.8), CVE-2023-5217 (v2: N/A, v3: 8.8, Cisco Security Risk Score: 100.0), CVE-2023-5129 (v2: N/A, v3: 9.6, Cisco Security Risk Score: 100.0), CVE-2023-5129 (v2: N/A, v3: N/A, Cisco Security Risk Score: N/A)	12: 12: 12:
Affected workloads:centos01	
Close	

Workloads Tab

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

💽 Cisc	co Secure Workload				⑦ Default → @ ~ ▲ ~ shole SECUI
=		You do not have an active license. The evaluation period will e	ind on Thu Nov 04 2021 03:41:29 GMT+0000. Take	action now.	
U Vulne	erabilities				
a CVS	S V2 DISTRIBUTION 🖌 Default 🗸				
•					
800-					
€00 - €			Access Complexity	Access Vector	Authentication
3 200 -					
× 0-	1 2 3 4 5	6 7 8 9 10	Availability Impact	Confidentiality Impact	Integrity Impact
4	412 Remotely Exploitable Low Complexity	814 Remotely Exploitable Higher Complexity	1241 Locally Exploitable Low Complexity	139	Locally Exploitable Higher Complexity
(Critical Severity	816 High Severity	1366 Medium Severity	424	Low Severity
CVEs	s Packages Workloads				
T	Workload 1	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	

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

Cisco Secure Workload						Tefaul	t • @~ L~
=	Workload Vulnera	bility Details - eg-	tet36-oracle7				
ul Vulnerabilities	31 vulnerable package	s (101 CVEs) on eg-tet3	36-oracle7				
CVSS V2 DISTRIBUTION - Default -		Package C\	/SSv2 Distribution Pac	kage CVSSv3 Distribution			
	10 -						
et a:o -	5-						
¢						s Vector	Authentication
400 -	0- N/A 1	2 3	4 5	6 7	8 9 10		
200 -			Packages C	ZVEs			
* 0- <u>1</u> 2 3 4	Package 1	Version 1	Worst Score (V2) ↓	Worst Score (V3)	CVEs 11	ality Impact	Integrity Impact
A 1 3 Remotely Exploitable	nspr	4.21.0-1.el7	10	9.8	CVE-2019-17006,CVE-2019-11		ploitable
4 I Z Low Complexity	nss	3.44.0-7.el7_7	10	9.8	CVE-2019-17006,CVE-2019-11	Higher Co	mplexity
Critical Severity	nss-softokn	3.44.0-8.0.1.el7_7	10	9.8	CVE-2019-17006,CVE-2019-11	121 Low Seve	
U Citucal Severity	nss-softokn-freebl	3.44.0-8.0.1.el7_7	10	9.8	CVE-2019-17006,CVE-2019-11	424	nty
CVEs Packages Workloads	nss-sysinit	3.44.0-7.el7_7	10	9.8	CVE-2019-17006,CVE-2019-11		
CVLS Packages Morkidaus	nss-tools	3.44.0-7.el7_7	10	9.8	CVE-2019-17006,CVE-2019-11		
Workload 14	nss-util	3.44.0-4.el7_7	10	9.8	CVE-2019-17006,CVE-2019-11	1	
eg-tet36-oracle7	python	2.7.5-89.0.1.el7	7.5	9.8	CVE-2021-3177,CVE-2019-209		
eg-tet36-centos7	python-libs	2.7.5-89.0.1.el7	7.5	9.8	CVE-2021-3177,CVE-2019-209		
eg-tet36-win19	grub2	2.02-0.87.0.1.el7	7.2	8.2	CVE-2020-25632,CVE-2020-25		
eg-tet36-win12r2			< 1 2 3	4 >			
eg-tet36-win10		ar ISON					
eg-tet36-win19-2	Download table data	i as Joury					

5 vulnerable packa	ges (96 CVEs)				
Pac	kage Cisco Security Risk Score Distr	bution	Package CVSSv2 Distributi	on Package CVSSv3 Distribution	
30 - 20 - 10 - 0 -	N/A	LOW	мер	IUM HIGH	
			Severity kages CVEs		
Package 1↓	Version↑↓	Worst (Cisco Security Risk Score ↑↓	Worst Severity (Cisco Security Risk Score) ↑↓	Wor
libaccountsservice	0.6.55-0ubuntu12~20.04.6	11		LOW	2.1
bind9-dnsutils	9.16.1-0ubuntu2.15	84		HIGH	N/A
bind9-host	9.16.1-0ubuntu2.15	84		HIGH	N/A
bind9-libs	9.16.1-0ubuntu2.15	84		HIGH	N/A
binutils	2.34-6ubuntu1.6	31		LOW	N/A
binutils-common	2.34-6ubuntu1.6	31		LOW	N/A
binutils-x86-64-lin	ux-gnu 2.34-6ubuntu1.6	31		LOW	N/A
curl	7.68.0-1ubuntu2.19	45		MEDIUM	N/A
gawk	5.0.1+dfsg-1	31		LOW	N/A
intel-microcode	3.20230808.0ubuntu0.20.04	4.1 28		LOW	N/A
1 2 3 4 Download table d	5 6 7 > ata as JSON _★ Download table da	ta as CSV			

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.

	Package Cisco Security Risk S	Score Distribution	Package C	VSSv2 Distri	bution	Package (VSSv3 Distri	bution	
0-									
	N/A	LOW	Sever Package:	-	MEDIUM			HIGH	
ackage †↓		Image/layer ↑↓				CVEs Î↓			
obrotli11	.0.7-2	docker.io/library	//wordpress/sl	ha256:c8713	c5be33	CVE-2020-8	927		
omagickwa	nd-6.q16-68:6.9.10.23+dfsg-2.	1+d docker.io/library	//wordpress/sl	ha256:fd468	125198	CVE-2021-2	0312, CVE-2	020-27751,	CVE-20
obsd00.9	9.1-2	docker.io/library	//wordpress/sl	ha256:dd99c	a928e71	CVE-2019-2	0367		
curses-bin-	6.1+20181013-2+deb10u2	docker.io/library	//wordpress/sl	ha256:f5600	c6330da	CVE-2022-2	9458, CVE-2	021-39537	
ozstd11.	3.8+dfsg-3	docker.io/library	//wordpress/sl	ha256:f5600	c6330da	CVE-2021-2	4031, CVE-2	021-24032	
ocom-err2-	1.44.5-1+deb10u3	docker.io/library	//wordpress/sl	ha256:f5600	c6330da	CVE-2022-1	304		
operl5.28	-5.28.1-6+deb10u1	docker.io/library	//wordpress/sl	ha256:7a17e	b00e8b	CVE-2011-4	116, CVE-20	20-16156	
patomic1	8.3.0-6	docker.io/library	//wordpress/sl	ha256:7a17e	b00e8b	CVE-2018-1	2886, CVE-2	019-15847	
oavahi-clie	nt30.7-4	docker.io/library	//wordpress/sl	ha256:5fbf3c	85f5b5f	CVE-2017-6	519, CVE-20	21-26720, C	VE-202
il-linux2	.33.1-0.1	docker.io/library	//wordpress/sl	ha256:f5600	c6330da	CVE-2022-0	563, CVE-20	21-37600	
1 2 3 lownload t		ad table data as CS\	/						

Figure 12: CVEs and Affected Packages in a Kubernetes Pod