

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 an	d 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.

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

٢	Cisco	o Secure Work	kload	CVE Det	ails - CVF-2018-	.8780				Default	● @~ ↓、 situle SECURE
ा ह	5 0 cves	Remotely Exploi Low Complexity Critical Severity Packages Wo	itable /	Reference I Affected pa 29.el7, ruby rubygems-2 Affected w	URL: https://access.n ickages: ruby-2.0.0.0 (gem-io-console-0.4, 2.0.14,1-29.el7 orkloads: collectorDa	edhat.com/security/cve/CN i48-29.el7, ruby-irb-2.0.0 2-29.el7, rubygem-json-1 tamover-1, collectorDatan	/E-2018-8780 .648-29.el7, ruby-libs-2.0 .7.7-29.el7, rubygem-psy nover-2	0.648-29.el7, rubygam-bigdec h-2.0.0-29.el7, rubygem-rdoc	:imal-1.2.0- :-4.0.0-29.el7,	C Locally Exploitable Higher Complexity	
Ě	T	CVE 11	Score (V2) ↓	Score (V3) 1↓	Severity (V2)	Base Severity (V3) ^{↑↓}	Access Vector (V2)	Access Complexity (V2)	Exploit Count 1	Authentication (V2)	Confidentiality Impact (V2)
44		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

Figure 5: Details for a CVE

٢	Cisco	o Secure Work	kload							Tofault	
≡				CVE Det	ails - CVE-2018-	-8780					
ш	5	Remotely Explo	itable /	Reference	URL: https://access.n	edhat.com/security/cve/C\	VE-2018-8780			Locally Exploitable Higher Complexity	
33 69	0	Critical Severity		Affected p 29.el7, ruby rubygems- Affected w	ackages: ruby-2.0.0.6 gem-lo-console-0.4 2.0.14.1-29.el7 orkloads: collectorDa	548-29.el7, ruby-irb-2.0.0 2-29.el7, rubygem-json-1 tamover-1, collectorDatan	0.648-29.el7, ruby-libs-2.0 1.7.7-29.el7, rubygem-psy nover-2	0.648-29.el7, rubygem-bigde ch-2.0.0-29.el7, rubygem-rdo	cimal-1.2.0- c-4.0.0-29.el7,	12 Low Severity	
e A	CVEs	Packages We	orkloads								
	T	CVE 1	Score (V2) ↓	Score (V3) †↓	Severity (V2)	Base Severity (V3) [†] ↓	Access Vector (V2)	Access Complexity (V2) 1	Exploit Count 🗍	Authentication (V2)	Confidentiality Impact (V2)
-44		CVE-2016-9587	9.3	8.1	HIGH	HIGH	NETWORK	MEDIUM		NONE	COMPLETE
<u> </u>		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

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

	Cisco	Secure Workload				💿 Default 👻	
			Package Details - rubygem-bigded	simal-1.2.0-29.el7		Vector	Authentication
ш	20 -		Package: rubygem-bigdecimal-1.2.0-29.el7				
8	0	1 2 3 4	CVEs: CVE-2017-10784 (v2: 9.3, v3: 5.4), C (v2: 7.5, v3: 5.6), CVE-2017-14064 (v2: 7.5, 2018-8780 (v2: 7.5, v3: 6.5), CVE-2018-100	ity Impact	Integrity Impact		
E., 18.	5	Remotely Exploitable Low Complexity	6.8, v3: 7.8), CVE-2019-8324 (v2: 6.8, v3: 7 0901 (v2: 6.4, v3: 6.5), CVE-2017-0900 (v2: 2018-1000073 (v2: 5, v3: 5.5), CVE-2018-1 v3: 5.3), CVE-2019-8322 (v2: 5, v3: 5.3), CV	 CVE-2018-16396 (v2: 6.8, v3: 5.9), CVE-2017-0898 (v2: 6.4, v3: 6.5), C S, v3: 4.3), CVE-2017-14033 (v2: 5, v3: 5.3), CVE-2018-8777 (v2: 5, v3: 7.4) 000075 (v2: 5, v3: 3.3), CVE-2018-1000077 (v2: 5, v3: 5.5), CVE-2019-832 CVE-2019-8323 (v2: 5, v3: 5.3), CVE-2018-8325 (v2: 5, v3: 5.3), CVE-2019-832 	VE-2017- 5), CVE- 1 (v2: 5, 7742 (v2:	Locally Exploitable Higher Complexity	
¢- ■	0	Critical Severity	5, v3: 4.7), CVE-2018-8778 (v2: 5, v3: 4.8), (v2: 4.3, v3: 6.1), CVE-2018-1000079 (v2: 4 Affected workloads: collectorDatamover-1,	CVE-2018-6914 (v2: 5, v3: 3.7), CVE-2018-8779 (v2: 5, v3: 3.7), CVE-2018 .3, v3: 5.5) collectorDatamover-2	-1000078	12 Low Severity	
*	CVEs	Packages Workloads					
	T	Package TI		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-2023-4575 (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-2023-4578 (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)	0 2: 2: 2:
Affected workloads:centos01	
Close	

Workloads Tab

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

۲	Cisco Secure Workload			The De	fault - @~ 1.~ diala SECURE
≡		You do not have an active license. The evaluation period will en	d on Thu Nov 04 2021 03:41:29 GMT+0000. Take a	iction now.	
ш	Vulnerabilities				
66 Re	CVSS V2 DISTRIBUTION - Default -				
æ	800 -				
۵	400		Access Complexity	Access Vector	Authentication
	200 -			-	
*	0- 1 2 3 4 5	8 7 8 9 10	Availability Impact	Confidentiality Impact	Integrity Impact
	412 Remotely Exploitable Low Complexity	814 Remotely Exploitable Higher Complexity	1241 Locally Exploitable Low Complexity	139 Local High	lly Exploitable ar Complexity
	O Critical Severity	816 High Severity	1366 Medium Severity	424 Low	Severity
	CVEs Packages Workloads				
	▼ Workload 11	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					Default - Q - L - Indus SECURE
=		Workload Vulnerability Details - e	g-tet36-oracle7			
<u> </u>	Vulnerabilities	31 vulnerable packages (101 CVEs) on eg-1	et36-oracle7			
60	CVSS V2 DISTRIBUTION + Default +	Package	CVSSv2 Distribution Pa	ckage CVSSv3 Distribution		
Π.		10 -				
86	800 -	5-				
۵	600 -	0-				s Vector Authentication
	200 -	NVA 1 2	3 4 5	t 7	8 9 10	
**	0-1234		Packages	CVES		ality Impact Integrity Impact
		Package 1 Version 1	Worst Score (V2) ↓	Worst Score (V3) 1↓	CVEs 1	
	412 Remotely Exploitable	nspr 4.21.0-1.el7	10	9.8	CVE-2019-17006,CVE-2019-11	130 Locally Exploitable
	- I Z Low Complexity	nss 3.44.0-7.el7_7	10	9.8	CVE-2019-17006,CVE-2019-11	Higher Complexity
	Critical Severity	nss-softokn 3.44.0-8.0.1.el7_7	10	9.8	CVE-2019-17006,CVE-2019-11	121 Low Severity
	0	nss-softokn-freebl 3.44.0-8.0.1.el7_7	10	9.8	CVE-2019-17006,CVE-2019-11	424
	CVEs Paskages Workloads	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	
	Y 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-2019-205	
	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					
	eg-tet36-win19-2	 Download table data as JSUN 				
		10			10	

Workload Vulnerabilit	y Details - node-1			Х
65 vulnerable packages (96	CVEs)			
Package C	isco Security Risk Score Distribu	tion Package CVSSv2 Distributi	on Package CVSSv3 Distribution	
30 - 20 - 20 - 10 -				
N/A	LC	W Severity MED Packages CVEs	лим нібн	
Package 1↓	Version 1↓	Worst Cisco Security Risk Score ↑↓	Worst Severity (Cisco Security Risk Score) ↑↓	Worst
libaccountsservice0	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-linux-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	3.20230808.0ubuntu0.20.04.1	28	LOW	N/A
< <tr> 1 2 3 4 5 6 3</tr>	7 > ISON <u>+</u> Download table data a	as CSV		
			C	lose

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 Dick S	core Distribution	Package	WSSv2 Diete	ibution	Package	VSSv3 Dietril	oution	
0-									
	N/A	LOW	Seve	rity es CVEs	MEDIUM			HIGH	
ackage Î↓		Image/layer †↓				CVEs 1↓			
obrotli11	.0.7-2	docker.io/library	//wordpress/	sha256:c8713	3c5be33	CVE-2020-8	927		
omagickwa	nd-6.q16-68:6.9.10.23+dfsg-2.1	+d docker.io/library	//wordpress/	sha256:fd468	f125198	CVE-2021-2	0312, CVE-20)20-27751, CVE	ē-20
obsd00.9	9.1-2	docker.io/library	//wordpress/	sha256:dd99	ca928e71	CVE-2019-2	0367		
curses-bin-	6.1+20181013-2+deb10u2	docker.io/library	//wordpress/	sha256:f5600	c6330da	CVE-2022-2	9458, CVE-20)21-39537	
ozstd11.3	3.8+dfsg-3	docker.io/library	//wordpress/	sha256:f5600	c6330da	CVE-2021-2	4031, CVE-20)21-24032	
com-err2-	1.44.5-1+deb10u3	docker.io/library	//wordpress/	sha256:f5600	c6330da	CVE-2022-1	304		
operl5.28	-5.28.1-6+deb10u1	docker.io/library	//wordpress/	sha256:7a17e	eb00e8b	CVE-2011-4	116, CVE-202	20-16156	
patomic1	8.3.0-6	docker.io/library	//wordpress/	sha256:7a17e	eb00e8b	CVE-2018-1	2886, CVE-20)19-15847	
bavahi-clier	nt30.7-4	docker.io/library	//wordpress/	sha256:5fbf3	c85f5b5f	CVE-2017-6	519, CVE-202	21-26720, CVE-	-202
il-linux2	.33.1-0.1	docker.io/library	//wordpress/	sha256:f5600	c6330da	CVE-2022-0	563, CVE-202	21-37600	
1 2 3 ownload t	4 5 6 7 14 >	d table data as CS\	/						

Figure 12: CVEs and Affected Packages in a Kubernetes Pod