# **Vulnerabilities Management**

This guide shows you how to mute vulnerabilities in Kiuwan Insights.

#### Contents:

- Vulnerabilities Management
  - Required Permissions
  - Scope of Mutes
- How to mute CVE vulnerabilities
  - Global Mutes Administration
    - By Vulnerability
    - By Component
  - Muting at the Component tab
  - Muting at the Security tab
  - Muting in Insights Management

# Vulnerabilities Management

As explained in Insights Security, Kiuwan Insights searches for vulnerabilities reported to the NIST National Vulnerability Database (NVD) (https://nvd.nist.gov/) that affect any of the external components being used by your application.

If Kiuwan finds any reported vulnerability of any component, it will display the details of the vulnerability and score the component in a **Security Risk indicator**.

But, depending on the specific case, the alert might not apply to your organization or you can decide not to be alerted about certain vulnerabilities.

In these cases, you can decide to mute the vulnerability so Kiuwan does not alert about it.

# **Required Permissions**

### Permissions

To mute vulnerabilities, only users granted with Application Management permission are allowed to access Mute Vulnerabilities modules.

# **Scope of Mutes**

Kiuwan Insights lets you mute a specific CVE over a component(s) (i.e. this specific component should not raise this specific CVE)

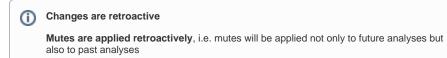
### You cannot completely mute a CVE.

You can mute a CVE over a specific component(s), but the CVE remains active and any new component affected by that CVE will still be reported.

#### Muting a vulnerability over a component can be applied to several scopes

Mute Scope	Precedence	Meaning
Global	1	The CVE muted applies globally to the selected component, i.e. to all the applications that component may appear.
Applicat ion	2	The CVE muted <b>applies to the selected component only in the</b> <b>specified application.</b> The same component in other applications remains flagged as vulnerable by that CVE.

The precedence column means the applicability of the mute in case of conflicts, being applied the case with higher precedence value.



# How to mute CVE vulnerabilities

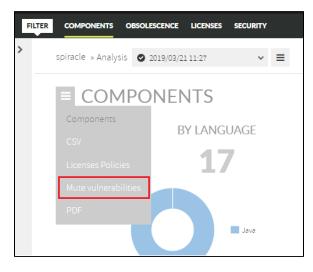
You can mute at different locations:

- Components tab (selecting a component row, and clicking on the Mute Vulnerabilities component's menu option)
- Security tab (selecting a CVE row, and clicking on the Mute Vulnerabilities menu option of any
  of the components affected by that CVE)
- Selecting Mute Vulnerabilities option at Components / Security tab's hamburger menu.
- Insights management section in the admin space

### **Global Mutes Administration**

Kiuwan Insights allows you to globally administrate the mutes defined within your Kiuwan account.

You can access the **Global Mute Admin** by selecting the Mute Vulnerabilities option at the Components / Security tab's hamburger menu.



Mute Vulnerabilities allows you to manage mutes based on Vulnerabilities and/or Components

🧋 ki	uwan code secura	Y CODE ANALYSIS	ARCHITECTURE		GOVERNANCE		puz	de 107
FILTER	COMPONENTS OBSOL	ESCENCE LICENSES	SECURITY				2019/02/24 - 2019/03/25 💊	ANALYZE
>	spiracle » Analysis 🧿	2019/03/21 11:27	× =					
	MUTE V	ULNERA	BILITIES					
	Choose what you want to se	ŵ.						
	By Vulner	shility	By Co	mpanent				
	Search by		bscore Impect Subscor	e CVSS v2 Base Scor	re Nute			
		٩	•	•	•			
								Clear
	OVE		CWE		Exploitability Subscore	Impact Subscore	CVSS v2 Base Score	Mute
	► CVE-2017-1000228		CINE-20		10	10		
	<ul> <li>CVE-2013-2115</li> </ul>		C///E-94		8.6	20	93 🖕	
	► CVE-2015-5211		CWE-20		8.6	20	93 💠	
	<ul> <li>CVE-2016-0785</li> </ul>		CINE-20			10		
	<ul> <li>CVE-2015-8315</li> </ul>		CWE-399		10	6.9	7.8 🔶	
	<ul> <li>CVE-2016-3092</li> </ul>		CWE-20		10	6.9	7.8 🜩	
	► CVE-2015-8858		CIVE-399		10	6.9	7.8 📫	_
	<ul> <li>CVE-2014-0107</li> </ul>		CIVE-264		10	6.4	7.5 🔷	
	CVE-2018-14718		CWE-502		10	6.4		

### By Vulnerability

When "By Vulnerability" tab is selected, the full list of Vulnerabilities discovered through all the applications of your Kiuwan account is displayed.

Click a CVE to open the list of components affected by that vulnerability.

¥ klawan соосзеляту соослидски наки				÷
CUITOM COMPONENTS PRIVATE VILVERABILITES MIT	TVALHEABLITIES LICENSE POLICIES			
MUTE VULNERABILITIES				
Choose what you want to see.				
By tuber billing	By Component			
Search by Equivability Subscenary imper-	et Subscore CISS Base Score Muse			
Chip Muteri				Citar
OF.	ove	Components	Exploitability Subscove in	spect Subscore CVSS Base Score
COE-2008-14721	CWE-513	2		6 <b></b>
Component	Vestion	Description		Nute
conflagment jackson comjectson-classified	28111	General data-binding functionality for Jackson works on tore treaming	E A PI	Modify
care factories package compactions-datationed	224	Denesi dale londing functionality for cacinate wards an aire streaming	Eva	woodfy

Click Modify in the component row to open the Mute Vulnerabilities dialog.

MUTE VULNERABILITIES			ж
Component comfacement jackson com jackson-databind	Version Language 23111 java	Description General descripting for Lassacri vorts on sone sometring HP	
CHE-2213-14721	CWE CVIE-202	Description Factors, polician-databilità 2x before 2.0.1 ingle allow remans attacken so conduct server ade request fogery (1584) attacka by leveraging fallar es block the allo2 jeves class flore polymorphic classe/allataba.	Severity
Mute: Scope Globel	Reson: None (default)	Comments: Lest modified by:	
Muter Scope Application	Reason:	Comments:	
*			×
CANCEL			SIVE

Then, you can decide to mute the vulnerability for the selected component either all applications, for a set of apps or only one application.

After muting, the scope of the mute is at the Mute Vulnerabilities tab.

сис. сис. 2008-14121	CNE ALLA		Components 1 🐔	Exploitability Subscare 2 9	Impact Solocove	C155 Base Score
Component com facen mi jackson com jackson-databind		Version 20111	Bescription General data-binding functionality for Jackson works on core covering	NP1	Hate N Application	Modify

### **By Component**

When **By Component** is selected, the full list of components affected by any CVE through all the applications of your Kiuwan account is displayed

Click a Component to open the list of CVEs found for that component.

📽 kiuwan соосысляту соосындлая маснта				
CUSTOM COMPONENTS HERATE VILLIGUALITES MUTEV	NEMBLINES UCENSIS POLICES			
MUTE VULNERABILITIES				
Choose what you want to see				
by intrachity	By Component			
Seech by Language Huse				
C Only Mused				Ceer
Component - com/leaterent/jectoon.com/jectoon-ideation/		wienbittes 48	1941300 2.8.4	Language Java
DE .	ONE	Explotability Subscore	Impact Subscore Cviti Ba	ne Score Mute
CVE-2028-L-0238	C/NE-902	19	5.9	2.1 🔹 Modify
0.0.2228-1988	220-2612	1.9		- 1.1 🗢 (MSSEV)
EVE 2020 1 K085	CN1.402	1.6	£+	L1 🤤 Modfy
0/5/2008-12814	C/HE-802		16	5.3 🤤 Modily
EVE-3258 14489	C/VE-002	10	16	
0/5/2225-14082	205-340	18	14	Nadly Modly

Clicking Modify for a CVE will open Mute Vulnerabilities dialog.

MUTE VULNERABILITIES								×
	Version Langue	PP			Description			
con faces ni jackson corejackson databied	-204 java				General class-binding/functionality for Jackson works on o	ore streaming API		
ONE		CWE		De	scription		Severity	
0/6-2218-14718		\$115,632		F# 10	tertifit, jusioon-dataland 2.x before 2.9.7 might allow remote attackers to evec block the sHy-ext class from polymorphic deserialization.	use articology code by leveraging failure	CANCE	
Mute: Scope Globel			Report.		Comments:	Last modified by:		
<ul> <li>mate for all applications</li> </ul>			Sone (default)	v				
Mute: Scope Application			Reason		Commercia	Last modified by		
🗆 kilovat-6877			None (defect)	٠				
C kissen-mezer			None (default)	¥				
⊖ kiosan-mili			None (default)	×				
() Nuver-seen			None (default)	¥				
C Tell_company			None (defect)	¥				
<		_						>
CANCEL								54472

Then, you can decide to mute the vulnerability for the selected component either for all applications, for a set of apps, or only for one application.

After muting, you will see the scope of the mute in the Mute Vulnerabilities tab.

н	Component		Whenebilities		Version		Longuege	
L	<ul> <li>com/lastecomi pacisan core pacison-dataland</li> </ul>		45 🗾		2.8.4		Java	
I	O/E	CWE		Exploitability Subscore	Impect Subscore	CVSS Base Scare	Huse	
I	016-2020-34730	CHE-902		10	5.3		K Clabol.	modify.

## Muting at the Component tab

Also, you can mute in the **Components** tab by clicking the **dropdown menu** at the right of a specific Component and selecting **Mute Vulnerabilities**.

kiuwan coocsecuerr coocanacras	URCION	GOVERNMENT					
COMPONENTS OBSOLISCINGS LICENSES BECK	NTY .					3156612-31569	10 V 1000
Kuvan-6877 x Analysis 🔹 2525-08/33.1234-develo	pres v 🗮						Î
COMPONENTS							
		1 DANGUAG	E	BY SECURITY RISK	KEEP IN MIND  Reconcentry		
	C		anne (m.) 7 generije	Crisk High Midan Now	8 expresent lan Orled annity 24 expression an vester with order		
Dealth by Longuage	nrth coeffict	disale *	Lovaria	1662/03/103 Mate	Caston *		Tex made Filt v
<ul> <li>Only Mused</li> </ul>							Ceer
Campanent		weekittes	Version	Flenama	Language	Obselescence Lisense risk risk	Security risk
	Deptered 0	4	111	sammons filespised 1,21 pr	ine.	Tableton Mass	20 C + C
commono-Neupload-commono-Neupload			2.8.4	action-deathind 2.5.4 pr	ing.	and the second second	
commons-file-pload-commons-file-pload     com/leasement/jackson.com/jackson-deablind		45	2.6.4	house-series of the			Not Line will be
		40	9234420151306	jety-http=8.1145/2010108.jet	Java	Manual Dataset	Multi Write Sche Mill De Moldfy Philoy

In the Mute Vulnerabilities dialog, select the CVE to Global Mute or Application Mute.

moorest		Version Language				
	od somme	ro-linulated 121 jan				
π	CHE	bestation		Scoor Global	Scoor Application	
n. (5-2234-0250		Belangson NubberGreen inve in Aasche Commons Filelipised before 131 as used in Aasche Tomost. Boss Web, and other products, allows remote attacken to	severcy	Global Mute	C Application	
		cause a denial of service (infinite loop and CPU consumption) via a crafted Content-Type header that bypesses a loop's intended exit conditions.		Resor	Response	
				None (default) v	None (default)	
				conneits:	commerco.	
5-2213-0248	\$115-354	The default configuration of Javassenie; consectamptinin Apache Commons Filia placed 1.0 through 1.2.2 uses the Amp directory for uplaced files, which		C Globel Mate	O Application Muta	
		allows local users to overwrite arbitrary files via an unspecified symitrix attack.		Reson.	Ferrors	
					none (default)	
				Connerts	Commercia	
5-2515-3992	CM#-20	The Highbordsheem class in Apache Common Filespland before 1.32, as used in Apache Tomost Til before T.3.11, 61, before 8.0.35, 8.51, before 8.0.35, and 52		C Gobel Nate	C Application Mute	
		before \$0.531/7 and other products, allows remote attackers to cause a denial of service (CPU consumption) via a long boundary string.	-	Report.	Ferrors	
				None (default)	None (default)	
				Comments	Commercia	
		Per Apeche: "Having swiewed your report we have porcluded that it does not represent a valid w/rembility in Apeche Commons Rie Uploed. If an application	_	C Gobel Nate	C Application Muter	

After clicking Save the muted vulnerability grays out when expanding the component.

Component		Valseabilities	Version	Filesame		Language	Obsolescence risk	License risk	Security risk
* commons-filespload commons-filespload		4 🛒1	121	commons-Neupland-1.2.1.jar		2010	1. Marcana	Here	<b></b>
Source									
<ul> <li>zkmenitor/pemanlorg.zkess.commem.zweb_version1.0</li> </ul>									
<ul> <li>MMSEL = org_plass.comman.pcommon _version 6.03</li> </ul>									
NAVEN - commons-Neupland:commons-Neupla	and version 12								
Valuesbäses									
CVE Wated C	OVE				Description				Severity
Cutu21140020 🧖 Crobel/Application C									
0.16.213.0248	2012-264				The default configuration of power service cont 12.2 costs the /tmp directory for uploaded file on unspecified symfrek attack.	lext.tempdir in Apache Di 11, which allows local use	ommons PileUplos rs 15 overvirite arb	d 13 through tracy files via	
0.6305300	265-28				The NublearEsteam class in Apache Commo before 7.078, 8x before 80.36, 8.5x before 8.5 remote attackers to cause a denial of service (	3, and 3. before 3.0.0 M	7 and other produ	cts, elleve	
CVE-0236-2000012 C	2012-2014				Per Apache "Having reviewed your report we winestability in Apache Commons Hie Opiaad source without fibering and/or validation that library a presented attacker might leverage"	I if an application determ	allow data from an	unavered	Gene

# Muting at the Security tab

The mute option is found also in the **Security** tab. Click a Vulnerability to display more details and the list of components affected by the vulnerability. At the bottom, in the Component section, click each dropdown button to mute vulnerabilities for each one of them.

Component	Muted	Version	Description	
	📕 Global			~
	Application			Mute Vulnerabiliti

There is a special case (as you can see below). It happens when there are two mutes for that CVEcomponent: it's muted by a Global mute and also by an Application mute. Then, there are two mutes, i.e. the component is muted for two reasons.

Component	Muted	Version	Description	
	K Global/Application			*

Whatever the mute reason, just select the **Mute Vulnerabilities** from the **dropdown menu** at the right of a specific Component.

Then, the Mute Vulnerabilities dialog opens.

MUT	e vul	NERAB	ILITIES					ж
	parsent	vok secur	Wentern Langunge ng neutrik program 111151.1542 juw					
CVE		CAE	Description	Severy.	Scope Clobel		Scope Application	
CVE-3		(). Spring Security Dilative writers 2.3 prior to 2.3.6, 1.2 prior to 2.2.5, 2.1 prior to 2.1.6, and 2.8 prior to 2.8.18, as well as older unsupported versions could be	-	🗋 Global Muta 🔅 Application		Application Nuse		
		susceptible to en-open redirector establishes can leaf an authorization code. A molicious user or establer can craft a request to the authorization endpoint, using the authorization code grent type, and specify a manipulated redirection URI via the redirect_url parameter. This can cause the authorization server to		Readors		Reapon:		
		redirect the resource owner scen-egent to a UR under the control of the attacker with the leaked authorization code.		None (default)		None (default)	÷	
					Comments		Convinents:	
					Last modified by:			
					wara.hemosa.or.2023/06/20			
¢								,
GANCE	L							sor

The Mute Vulnerabilities dialog lets you select the CVE to mute and decide **Global Mute** or **Application Mute**.

# **Muting in Insights Management**

Open the drop-down menu on the upper-right corner and select Insights Management

	~				
2023/05/22 - 2	Audits Management				
	Models Management				
	Reports Management				
	Account Management				
	Application Management				
	Users Management				
	Insights Management				
	Activity				
	Documentation				
	Download Kiuwan Local Analyzer				
	Log Out				

The Mute Vulnerabilities page displays:

📌 kluwan 🛛 🕬	CODEMANDER I	NIN URCICLE	CONTINUE O INSIGHTS				•
CUITON COMPO	MENTS PRIVATE VALVERABILITIES	MITTVAHEMBLITES	LOWERNOOR				
MUTE VU	LNERABILITIES						
Crocke what you want to	5 30W.						
	By Talmendality		By Component.				
Genrofi by	Explosibility Subserve	Impect Subscore	CHSS Brow Scove Muse				
Coly Mused							Cirar-
C/E		OVE		Components	Exploitability Subscove	Impect Subscore	CVSS Base Score
* CVE-2018-14721		CNE-818		1	2		
	on core jackson-classified on core-jackson-classifierd		Version 28111 284	Desception General data-binding functionality for Jackson: works on tare toos two each data-binding functionality for Jackson works on tare toos		8429	Modily

Please follow the instructions mentioned in the steps before to mute vulnerabilities.