

Custom Components

Custom Components

Contents

- [Custom Components](#)
 - [Required Permissions](#)
 - [How to manage components in Kiuwan Insights](#)
 - [Remove custom attribute](#)
 - [Modify custom data](#)
 - [Modify licenses](#)
 - [Delete Component](#)
- [How to manage private vulnerabilities in Kiuwan Insights](#)
- [Edit custom components, private vulnerabilities, and licenses associated to custom components by the customer](#)
 - [Insights Components](#)
 - [Insights Obsolescence](#)
 - [Insights Licenses](#)
 - [Insights Security](#)

A customer will be able to add, modify, and delete custom components. Also, adding their own information about private vulnerabilities and licenses associated with custom components.

The customer can add components to Kiuwan, which may be custom or not. A custom component should be custom when the customer is the component owner or is a modification of the other public component.

For example a custom component may be:

- Group name: `com.my.component`
- Artifact name: `component-core`
- Version: `1.0.0`
- Language: `java`

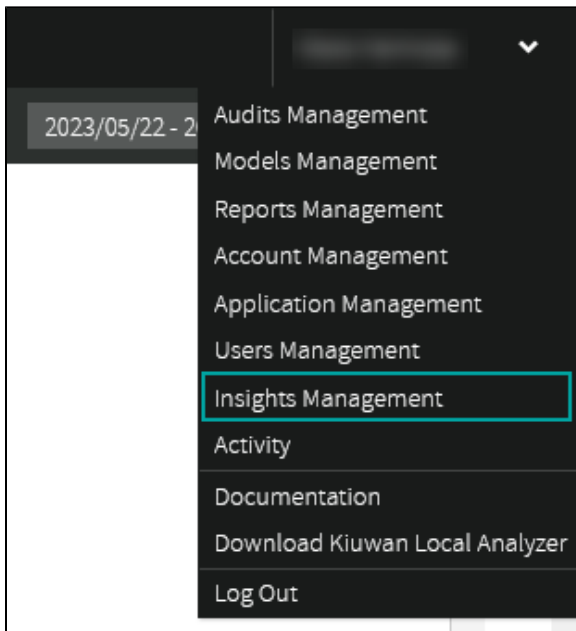
Required Permissions

Only users granted with Application Management permission are allowed to access Policies Management modules, add custom components, private vulnerabilities, or associate licenses to custom components.

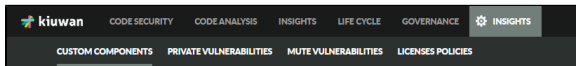
How to manage components in Kiuwan Insights

You can manage components using the REST API defined below Insights Custom Components: <https://static.kiuwan.com/rest-api/kiuwan-rest-api.html>
Another way is through the Kiuwan website.

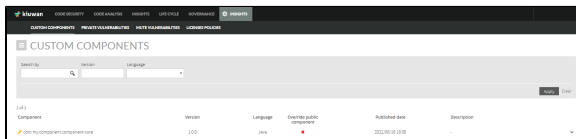
1. Go to **Insights Management** in the setting menu.



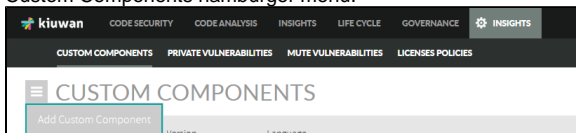
2. Select **Custom Components**.



Below, the custom components administration in the Kiuwan website:



3. You can add new custom components by selecting **Add Custom Component**, located at the Custom Components hamburger menu.



4. In the **Add Custom Component** screen, fill the custom component data form.



The mandatory fields in the ADD CUSTOM COMPONENT form are "Artifact Name," "Version," "Language," and "Published date."

- **Show reported public component vulnerabilities:** If you check this option, the public vulnerabilities found by Kiuwan will be shown in the Kiuwan analysis that contains these components and the security risk will be calculated with these vulnerabilities and the private vulnerabilities.
- **Apply default licenses:** If you check this option the licenses found by Kiuwan will be shown in the Kiuwan analysis that contains these components and the license risk will be calculated with these licenses and the licenses associated by the customer.

5. Click **Save**.

In the list of custom components you have the following actions:

- **Remove custom attribute:** Removes the custom attribute, but the component will still exist and the data could be replaced by the public data if the component is public.
- **Modify custom data:** Updates the custom components data.
- **Modify licenses:** Modify associated licenses to custom components.
- **Delete component:** This option is enabled if no public component with the same group name, artifact name, version, language exists. Also, if the component has not an analysis.

Component	Version	Language	Overrids public component	Published date	Description	
com.kiuwan:kiuwan-components-features	1.0	java	✓	2020/05/01 00:00	kiuwan-components	⌵
com.kiuwan:kiuwan-components-features	1.0	java	✓	2020/05/01 00:00	kiuwan-components	⌵
com.kiuwan:kiuwan-components-features	1.0	java	✓	2020/05/01 00:00	kiuwan-components	⌵
com.kiuwan:kiuwan-components-features	1.0	java	✓	2020/05/01 00:00	kiuwan-components	⌵
com.kiuwan:kiuwan-components-features	1.0	java	✓	2020/05/01 00:00	kiuwan-components	⌵

Remove custom attribute

This action removes the custom attribute, but the component will still exist and the data could be replaced by the public data if the component is public.

Modify custom data

The option “Modify licenses” modifies associated licenses to custom components. If you select this option a pop-up opens where you could modify the licenses associated to custom components.

Modify licenses

The option “Modify licenses” helps you modify associated licenses to custom components. If you select this option a pop-up opens where you can modify the licenses associated to custom components.

Component	Version	Language	Apply default licenses	Published date	Description	
com.kiuwan:kiuwan-components-features	1.0	java	⌵	2020/05/01 00:00	kiuwan-components	⌵
License	SPDX license	Type	URL		Risk	
Apache License 2.0	Apache 2.0	Permissive	https://www.apache.org/licenses/LICENSE-2.0.html		Low	⌵
MIT License	MIT	Permissive	https://www.mit.edu/~newman/opensource/		Low	⌵
GNU General Public License v3.0 only	GPL v3.0	Copyleft	https://www.gnu.org/licenses/gpl-3.0.html		High	⌵
Add license	xxx					⌵
License	SPDX license	Type	URL		Risk	
Apache License 2.0	Apache 2.0	Permissive	https://www.apache.org/licenses/LICENSE-2.0.html		Low	⌵
MIT License	MIT	Permissive	https://www.mit.edu/~newman/opensource/		Low	⌵

- You can delete associated licenses by the customer or add new licenses, and select if you want to apply for default licenses or not. To delete associated licenses you must click **Delete** located next to the Risk column.
- Search for new licenses in the Add license search box, and select the licenses by clicking **Add** located next to the Risk column.
- After you finished modifying the licenses component, click **SAVE**.

Delete Component

This option will be enabled if does not exist a public component with the same group name, artifact name, version, and language, and the component has not in an analysis

This option deletes the component and will not appear in the obsolescence data for other components with the same group name, artifact name, and language.

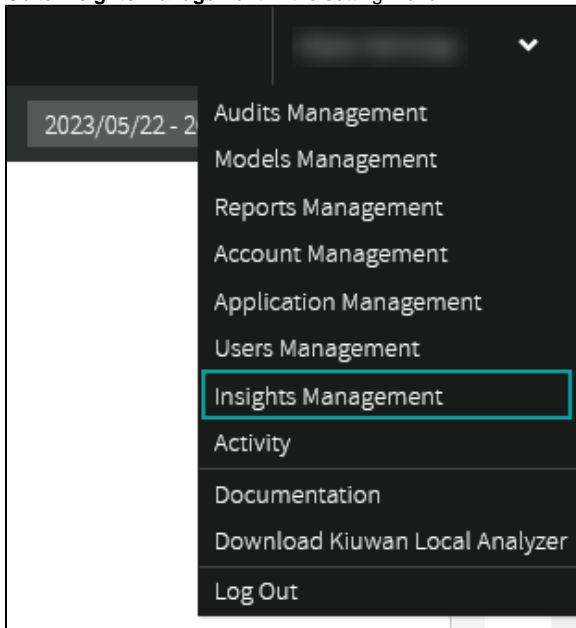
How to manage private vulnerabilities in Kiuwan Insights

You can manage components using the REST API defined below Insights Custom Components: <https://static.kiuwan.com/rest-api/kiuwan-rest-api.html>

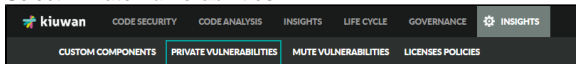
Another way is through the Kiuwan website.

You must go to Insights Management in the setting menu:

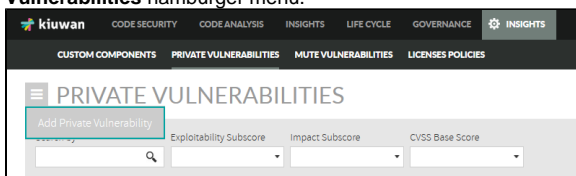
1. Go to **Insights Management** in the setting menu.



2. Select **Private Vulnerabilities**.



3. You can add new private vulnerabilities by selecting **Add Private Vulnerability** at the **Private Vulnerabilities** hamburger menu.



4. In the **Add Private Vulnerability** screen, fill the private vulnerability data form.

A screenshot of the 'ADD PRIVATE VULNERABILITY' form. The form includes fields for Vulnerability Code, CWE, Description, Exploitability Subscore, Impact Subscore, and CVSS v2 Base Score. Below these fields is a section for CVSS v2 Base Score details, including a Vector field and two columns of metrics: Exploitability Metrics (Attack Vector (AV), Access Complexity (AC), Authentication (Au)) and Impact Metrics (Confidentiality Impact (C), Integrity Impact (I), Availability Impact (A)). Each metric has a dropdown menu for selection. At the bottom, there are 'CANCEL' and 'SAVE' buttons.

Vulnerability code (Mandatory, CWE, and Description): The vulnerability code must be unique.

A screenshot of the 'ADD PRIVATE VULNERABILITY' form, focusing on the top section. It shows the 'Vulnerability Code' field, the 'CWE' dropdown menu, and the 'Description' text area. The 'Exploitability Subscore', 'Impact Subscore', and 'CVSS v2 Base Score' dropdowns are also visible.

CVSS v2 section: You can inform the CVSS v2 attack vector for the current private vulnerability.

A screenshot of the 'CVSS v2 Base Score' section of the form. It shows the 'Vector' field and two columns of metrics: Exploitability Metrics (Attack Vector (AV), Access Complexity (AC), Authentication (Au)) and Impact Metrics (Confidentiality Impact (C), Integrity Impact (I), Availability Impact (A)). Each metric has a dropdown menu for selection. At the top left of this section, there is a link that says 'Hide CVSS v2 Data'.

When you select all the data, the score and sub-score are populated.

Vulnerability Code	CWE	Exploitability Subscore	Impact Subscore	CVSS Base Score
		4.1	5.4	4.7

Description:

[Hide CVSS V2 Data](#)

CVSS v2 Base Score: 4.7

Vector: (AV:A/AC:L/Au:M/C:P/I:P/A:P)

Exploitability Metrics: 4.1

Attack Vector (AV): Local (AV:L) **Adjacent Network (N/A)** Network (AV:N)

Access Complexity (AC): High (AC:H) Medium (AC:M) **Low (AC:L)**

Authentication (Au): Multiple (Au:M) Single (Au:S) None (Au:N)

Impact Metrics: 6.4

Confidentiality Impact (C): None (C:N) **Partial (C:P)** Complete (C:C)

Integrity Impact (I): None (I:N) **Partial (I:P)** Complete (I:C)

Availability Impact (A): None (A:N) **Partial (A:P)** Complete (A:C)

CVSS v3 section: You can inform the CVSS v3 attack vector for the current private vulnerability.

[Hide CVSS V3 Data](#)

CVSS v3 Base Score:

Vector:

Exploitability Metrics:

Attack Vector (AV): Network (AV:N) Adjacent Network (AV:A) Local (AV:L) Physical (AV:P)

Attack Complexity (AC): Low (AC:L) High (AC:H)

Privileges Required (PR): None (PR:N) Low (PR:L) High (PR:H)

User Interaction (UI): None (UI:N) Required (UI:R)

Scope (S): Unchanged (S:U) Changed (S:C)

Impact Metrics:

Confidentiality Impact (C): None (C:N) Low (C:L) High (C:H)

Integrity Impact (I): None (I:N) Low (I:L) High (I:H)

Availability Impact (A): None (A:N) Low (A:L) High (A:H)

Affected components and versions:

a. Click **Add Component** to add a new affected component.

Group Name	Artifact Name	Language	Affected Versions
Add Component			

b. Fill the component information in the available fields. Below, you will find more information of how to fill the **Affected Versions**.

Group Name	Artifact Name	Language	Affected Versions
			<input type="checkbox"/> Is fixed version <input type="checkbox"/> Initial version <input type="checkbox"/> Included <input type="checkbox"/> End version <input type="checkbox"/> Included
Add Component			

Take into account that the **Artifact Name** and **Language** fields are mandatory.

The affected versions can be fixed versions or range versions:

- **Fixed Version:** You must check the **Is fixed version** checkbox and enter the **Field version**.

Group Name	Artifact Name	Language	Affected Versions
			<input checked="" type="checkbox"/> Is fixed version <input type="checkbox"/> Initial version <input type="checkbox"/> Included <input type="checkbox"/> End version <input type="checkbox"/> Included
Add Component			

- **Range Version:** You must uncheck the **Is fixed version** checkbox and enter the **Initial version**.

Group Name	Artifact Name	Language	Affected Versions
			<input type="checkbox"/> Is fixed version <input checked="" type="checkbox"/> Initial version <input type="checkbox"/> Included <input type="checkbox"/> End version <input type="checkbox"/> Included
Add Component			

If the initial version is included you must check the **Included** checkbox.

Group Name	Artifact Name	Language	Affected Versions
			<input type="checkbox"/> Is fixed version <input type="checkbox"/> Initial version <input checked="" type="checkbox"/> Included <input type="checkbox"/> End version <input type="checkbox"/> Included
Add Component			

If the private vulnerability affects all versions from the initial version you must leave the **End Version** field empty.

Group Name	Artifact Name	Language	Affected Versions
			<input type="checkbox"/> Is fixed version <input type="checkbox"/> Initial version <input type="checkbox"/> Included <input type="checkbox"/> End version <input type="checkbox"/> Included
Add Component			

If the private vulnerability has end affected version, fill the **End version** field and if the end version is included in vulnerable versions you must check the **Included** checkbox.

Group Name: Artifact Name: Language: Affected Versions: ☐ Initial version ☐ Included ☐ End version ☐ Included ☐

You can add **Affected version** or **Delete affected component**.

Group Name: Artifact Name: Language: Affected Versions: ☐ Initial version ☐ Included ☐ End version ☐ Included ☐

If you select **Add Affected Version** a new affected version for this component will display.

Group Name: Artifact Name: Language: Affected Versions: ☐ Initial version ☐ Included ☐ End version ☐ Included ☐

Also, you can **Delete affected versions**.

Group Name: Artifact Name: Language: Affected Versions: ☐ Initial version ☐ Included ☐ End version ☐ Included ☐

5. After completing to configure your private vulnerability information, click **SAVE**.


In the list of private vulnerabilities you have the following actions:

- Modify vulnerability
- Delete vulnerability

Vulnerability Code	CVE	Applicable to	Impact	CVE Base Score	Description
10001	CVE-2019-1111	Low	Low	2.2	Low
10002	CVE-2019-1111	Low	Low	2.2	Low
10003	CVE-2019-1111	Low	Low	2.2	Low
10004	CVE-2019-1111	Low	Low	2.2	Low
10005	CVE-2019-1111	Low	Low	2.2	Low
10006	CVE-2019-1111	Low	Low	2.2	Low
10007	CVE-2019-1111	Low	Low	2.2	Low
10008	CVE-2019-1111	Low	Low	2.2	Low
10009	CVE-2019-1111	Low	Low	2.2	Low
10010	CVE-2019-1111	Low	Low	2.2	Low

Edit custom components, private vulnerabilities, and licenses associated to custom components by the customer

Insights Components


Next to the custom components, the following icon  is displayed. Also, the following risks are displayed depending on the custom data:

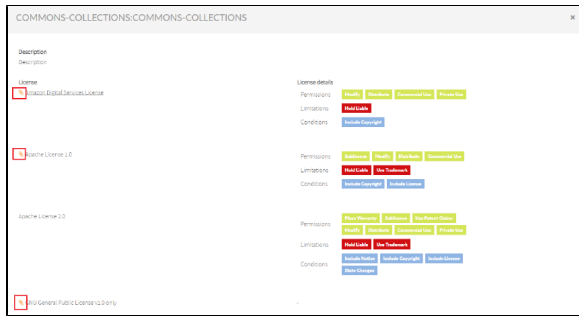
- **Obsolescence risk:** Depends on the component date and other custom components with the same group name, artifact name, and language.
- **License Risk:** Depends on the licenses found by Insights for this component, if you have checked this option, and the associated licenses by the customer.
- **Security Risk:** Depends on the vulnerabilities found by Insights for this component, if you have been checked this option, and the private vulnerabilities affecting this component.




Also, you can filter by **Custom** components:

Search by: Language: Initial version: Obsolescence risk: License risk: Security risk: Status:


The associated licenses are represented by the  icon.



And the private vulnerabilities that affected this component are represented by the  icon.



Insights Obsolescence

Next to the custom components, the  icon is displayed. Also, obsolescence risk depends on the custom data:

- Depends on the component date and other custom components with the same group name, artifact name, and language.

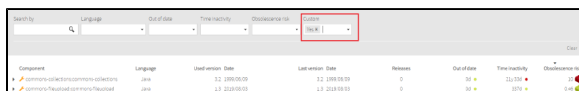
If the component is a copy of another public component when you display the drill-down you can see the public data for this component:




You can see the timeline for the public component:



Also, you can filter by **Custom** components.



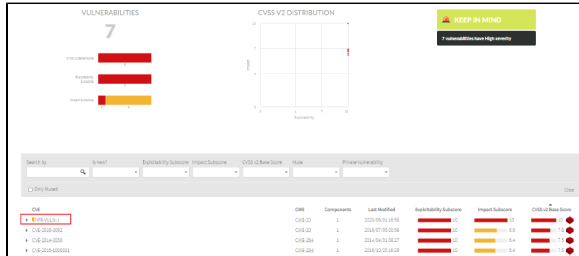
Insights Licenses

The custom components with licenses associated by the customer have the  icon next to the component name:

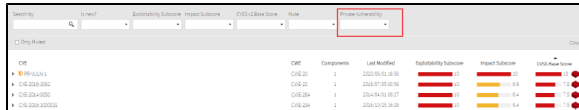



Insights Security

The private vulnerabilities have the  icon next to the vulnerability name.



Also, you can filter by **Private Vulnerabilities**:



The custom components affected by private vulnerabilities displays  next to the component name:

