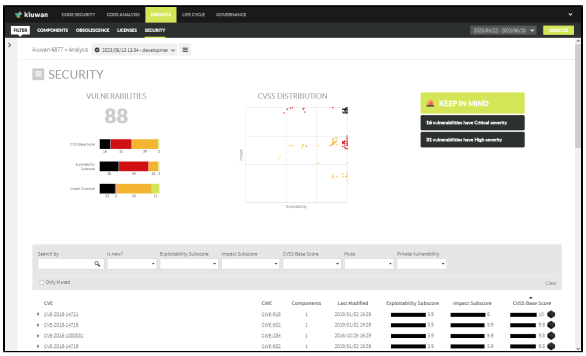
Insights Security

This section introduces you to the **Security** tab in Kiuwan Insights.

Contents:

Security in Kiuwan Insights

Go to **Insights** > **Security** to view security information on vulnerabilities found in components.



The main screen of the Security tab shows first-hand information on the Vulnerabilities, the CVSS Distribution chart, and a summary of the number of vulnerabilities with Critical and High severity. In addition, you can find the list of all the analysis vulnerabilities. To find a CVE, you can refine your search by using the filter based on the search criteria described below:

- **Search by:** Type any reference of search.
- **Is New?:** Select **Yes** if the vulnerability is new; otherwise, select **No**.
- **Exploitability Subscore:** Depending on the severity of the exploitability subscore, select **Critical** , **High**, **Medium**, **Low**, or **None**.
- **Impact Subscore:** Select **Critical**, **High**, **Medium**, **Low**, or **None** depending on the severity of the impact subscore.
- **CVSS Base Score:** Based on your search preference, select **Critical**, **High**, **Medium**, **Low**, or **None**.
- **Mute:** Refine your search to the muted components by selecting **Global**, **Application**, **Global /Application**, or **None**.
- **Private Vulnerability:** Filter your search by private vulnerabilities.

Security Risk

For every external component, Kiuwan Insights searches for vulnerabilities reported to public vulnerability databases such as the **NIST National Vulnerability Database (NVD)** and others.

If Kiuwan finds any reported vulnerability in your component, it displays the details of the vulnerability and scores the component with a **Security Risk indicator.**

Security Risk Indicator

A component's **Security Risk** is based on **Base Scores** (**Severities)** of its vulnerabilities:

- If the selected component has more than one vulnerability, Kiuwan will label the component with the highest severity value of all the vulnerabilities of the component.
- If the selected component has only one vulnerability, the Severity of that vulnerability will be the Security Risk of the component.

The Security Risk indicator of a component is represented with the following labels:

CVSS

Kiuwan Insights supports the calculation of the vulnerability security score for the components using NIST Common Vulnerability Scoring System (CVSS). The CVSS method is used to provide a value of severity.

Kiuwan calculates the CVE's scores using CVSS v3, and using CVSS v2 only when v3 is not available. Below you can find more information on the two versions:

- CVSS v2
- CVSS v3

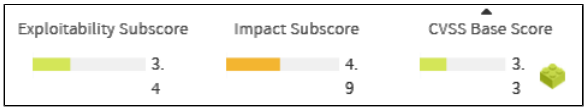
Common Vulnerability Scoring System (CVSS) v2

For every vulnerability, CVSS v2 provides an overall **Base Score** that "represents the intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments" (https://www.first.org/cvss/v2/guide)

CVSS v2 Base Score

The **Base Score** is based on the two main characteristics (modeled as Subscores) of any vulnerability (with associated metrics):

- **Exploitability Subscore**: the degree of difficulty to access and exploit the vulnerability
- **Impact Subscore**: if exploited, how important would be the consequences



The Base Score, as well as Exploitability and Impact subscores, are displayed as a numeric range from 0 to 10, with an associated color based on its importance ("the higher, the worse").

CVSS v2 Scores	
Value	**Label**
[0, 4]	Low
[4, 7]	Medium

[7, 10]	High

Exploitability and Impact subscores are calculated from their associated metrics.

Kiuwan Insights displays the value for every subcore's metric. Below you can find the meaning for every metric but, as a rule of thumb, you can consider that the more to left the value of the metric is, the more dangerous the vulnerability is:

Exploitability metrics

- **Attack Vector** (AV): This metric reflects the level of proximity the attacker needs to obtain to the system to exploit the vulnerability. The more remote an attacker can exploit the vulnerability, the more vulnerable the system is.
  - Values: Local - Adjacent - Network (L / A / N)
- **Access Complexity** (AC): Once the target system is reached, this metric reflects the complexity required to exploit the vulnerability (relative to the existence of barrier conditions). The easier to exploit the vulnerability, the more vulnerable the system is.
  - Values: Low – Medium – High (L / M / H)
- **Authentication** (Au): This metric reflects the number of times the attack needs to authenticate before being able to exploit the vulnerability. The fewer times he needs, the more vulnerable the system is.
  - Values: Multiple – Single – None (M / S / N)

Impact metrics

- **Confidentiality Impact** (C): This metric reflects the degree to which the vulnerability can read system data and produce confidential information disclosure to non-authorized users.
  - Values: None - Partial - Complete (N / P / C)
- **Integrity Impact** (I): This metric reflects the degree in which the vulnerability allows the attacker to modify existing system data, compromising the trust and veracity of data.
  - Values: None - Partial - Complete (N / P / C)
- **Availability Impact** (A): This metric reflects the degree to which the vulnerability affects the availability and use of the system.
  - Values: None - Partial - Complete (N / P / C)

Values of the above metrics are combined to calculate CVSS v2 Base Score and Exploitability / Impact Subscores as described at https://nvd.nist.gov/vuln-metrics/cvss/v2-calculator

Common Vulnerability Scoring System (CVSS) v3

CVSS v2 has evolved to v3 (https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator) introducing changes to metrics (new metrics and different possible values).

CVSS v3 Base Score

The **Base Score** for CVSS v3 is presented as a number ranging from 0 to 10, with an associated color based on its importance ("the higher, the worse").

CVSS v3 Scores	
Value	**Label**
[0, 4]	Low
[4, 7]	Medium
[7, 9]	High
[9, 10]	Critical

Kiuwan Insights displays the value for every subscore's metric. Let's examine the meaning of every metric.

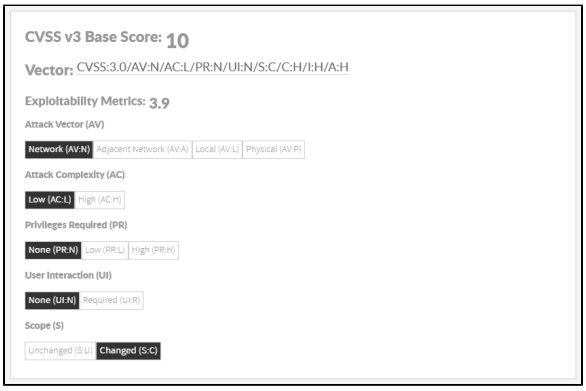
Exploitability metrics

- **Attack Vector** (AV): This metric reflects the level of proximity the attacker needs to obtain to the system to exploit the vulnerability. The more remote an attacker can exploit the vulnerability, the more vulnerable the system is.
    - Values: Network - Adjacent Network - Local - Physical (N / A / L / P)
- **Attack Complexity** (AC): This metric delineates the attacker's out-of-control conditions that must exist to exploit the vulnerability. For less complex attacks, the metric value is greater.
    - Valued: Low - High (L / H)
- **Privileges Required** (PR): This metric presents the attacker's required privileges in order to exploit the vulnerability successfully. The greater the metric, the fewer privileges are required. For less required privileges, the metric value is greater.
    - Values: Low – Low – High (N / L / H)
- **User Interaction** (UI): This metric describes how much interaction of the user is needed before the vulnerability can be exploited. The metric value is greater for less required user interaction.
    - Values: None - Required (N / R)
- **Scope** (S): The computing authority determines a set of privileges when granting access to the resources of a computer. The change of Scope occurs when the vulnerability of a component ruled by one authorization scope affects resources that are ruled by another authorization scope.
    - Values: Unchanged - Changed (U / C)

Impact Metrics

- **Confidentiality Impact** (C): This metric calculates the degree of confidentiality loss caused by an exploited vulnerability.
    - Values: None - Low - High (N / L / H)
- **Integrity Impact** (I): This metric calculates the degree of integrity loss caused by an exploited vulnerability.
    - Values: None - Low - High (N / L / H)
- **Availability Impact** (A): This metric calculates the degree of availability loss caused by an exploited vulnerability.
    - Values: None - Low - High (N / L / H)

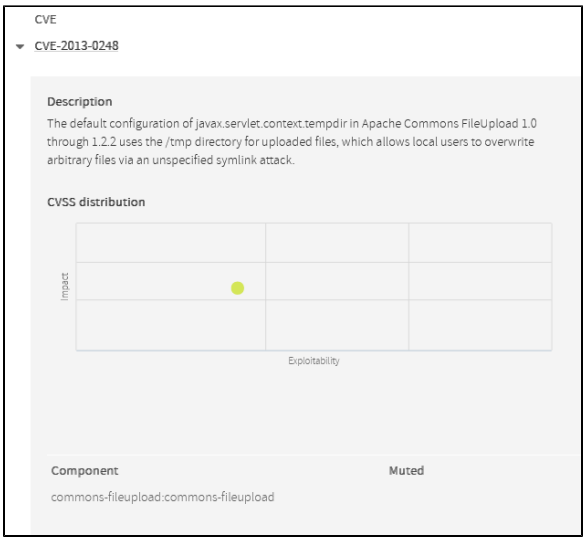
Values of the above metrics are combined to calculate CVSS v3 Base Score and Exploitability / Impact Subscores as described at https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator.



CVSS Distribution 2-axis figure

Each listed CVE provides a vulnerability description and the CVSS Distribution 2-axis figure. This figure can help you visualize two main characteristics of the vulnerability.

- The closer to the right a vulnerability is, the easier it will be to exploit it.
- The closer to the top the vulnerability is, the consequences will have a higher impact.



New vulnerabilities

The NIST database is continuously being feed with new vulnerabilities.

Do not worry if, after the date you run the analysis, new vulnerabilities are found that affect some of your components. Kiuwan Insights is continuously inspecting the NIST database for new vulnerabilities.

If there are new vulnerabilities that affect some of the components of your app, those components will display those new vulnerabilities (marked as **New**) without the need to run a new analysis.

Kiuwan will keep your components inventory up-to-date without the need to run new analyses.