Exploits

Exploits detail the ways in which a vulnerability can be taken advantage of by stealing data or otherwise inflicting harm on an organization. Visibility of the number and types of exploits facilitates the prioritization of vulnerabilities. The **Exploits** page shows exploits that have been imported into RiskVision.

Exploits are usually mapped to vulnerabilities through CVEs, although the exploit may have additional identifiers it is mapped to, depending on the data source.

Exploits is a grid available in the **Vulnerabilities** menu, which is visible only if you possess the Threats and Vulnerabilities View permission. This grid contains exploits imported from the **Administrator** application.

The Exploits grid.

> The **Date Added** and **Last Updated Date** columns are not default. They can be added by using the **Customize** action from the **More Actions** dropdown.

To expand an exploit:

1. Open the **Vulnerabilities** menu.

2. Click the **Exploits** page and click an exploit to open.

The Exploits Details page.

The following table summarizes different tabs available in the **Exploits Details** page:

Tab	Description
General	Displays detailed exploit information, including the name, description, platform, type of exploit, port used by the exploit, CVEs the exploit maps to, the date the exploit was published or submitted, and the dates the exploit was added and last updated.
Vulnerabilities	Displays the vulnerabilities associated with the exploit. • Vulnerabilities by Identifier: Displays the following columns: Identifier, Severity, CVSS Score, Total Entities, Without Tickets, and Without Patches. • Vulnerabilities by Entity Criticality: Displays the Entity Criticality, Total Affected, and Without Tickets.