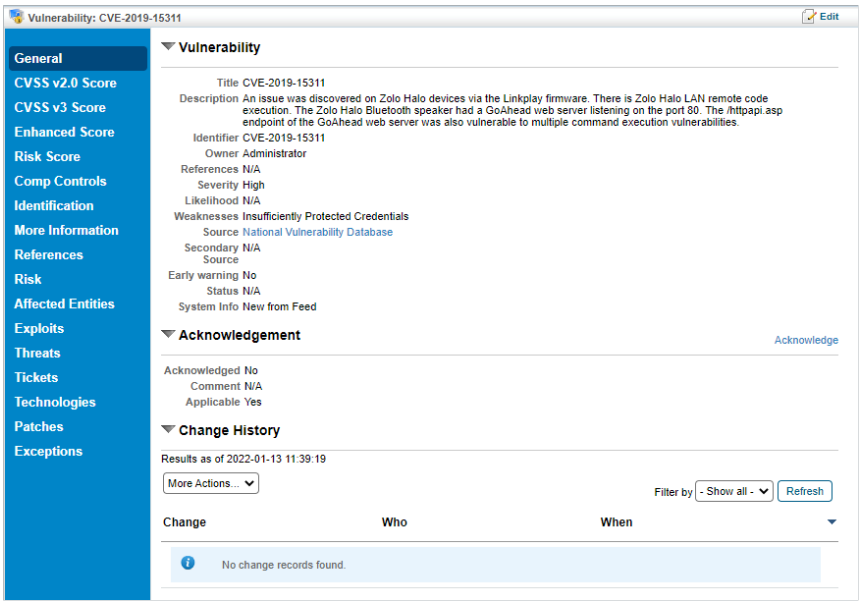
Vulnerability Details Overview

The **Vulnerability Details** page contains assorted information to help you manage your remediation effort. This page contains a series of tabs that are used to:

- Acknowledge vulnerabilities to mark them as applicable or duplicate;
- Provide substantiation to remediate, examine, or work around vulnerabilities; and
- Create tickets to resolve related vulnerability instances. Vulnerability instances represent the individual occurrences of the vulnerability on each affected entity.

To expand a vulnerability:

1. Open the **Vulnerabilities** menu.
2. Click any page, such as **My Vulnerabilities, Vulnerabilities from Scanners or Users**, or **Inferred Vulnerabilities**.
3. Select a vulnerability.



The Vulnerability Details page.

To update the information available on the various tabs of the **Vulnerability Details** page, you must have the Threats and Vulnerabilities View and Threats and Vulnerabilities Update permissions. The following table summarizes the different tabs available in the **Vulnerability Details** page.

TAB	DESCRIPTION
General	Displays information, such as severity, likelihood, and source. Allows users to assign an owner and status to the vulnerability.
CVSS v2.0 Score	The Common Vulnerability Scoring System is an open framework for communicating the characteristics and impacts of IT vulnerabilities. RiskVision displays each vulnera base score, impact, and exploitability sub-scores, as well as the temporal and environmental scores.
CVSS v3 Score	CVSS v3 will provide a better indication of the relative severity of vulnerabilities, because it better reflects the true impact of the vulnerability being rated in software cc middleware. The title of this tab's page, as well as its score sections, will be displayed as either 3.0 or 3.1 depending on the vulnerability's CVSS version.
Enhanced Score	Displays the Enhanced Score of a vulnerability. For scanner-reported vulnerabilities, it is not uncommon that the vulnerability will map to multiple CVE's. When this hap lines, one for each mapped CVE, and the Enhanced Score will be the sum of the Enhanced Scores for each of the mapped CVE's.
Risk Score	Displays all of the input vectors used to calculate the Entity Criticality Factor in columns, with their appropriate values. Also displays the Vulnerability Risk Factor and re the following levels: • Risk Score of vulnerability instance • Risk Score of vulnerability definition • Risk Score of an entity This tab uses all possible groupings of the Risk Score formula that use Entity Criticality to calculate the Entity Criticality Factor portion of the Current Risk Score.
Comp Controls	Displays all of the vulnerability compensating controls attached to a vulnerability. Allows users to add existing controls to a vulnerability and to edit the detection and p
Identification	Provides vulnerability IDs that have been identified together for a vulnerability, such as when you're using multiple scanners.
More Information	Shows attached information using the rich text editor interface to provide more information related to the vulnerability, such as how it affects your organization and any a
References	Shows mapped vulnerabilities to organization and industry-defined controls.
Exploits	Displays exploits linked to vulnerabilities.
Risks	Displays risks associated with vulnerabilities in your environment.
	Shows the entity groups that have technology affected by the vulnerability. These groupings are defined in Threat Management Preferences. To view specific entities, se You can create a ticket or add to an existing ticket for entities collections on this tab.

Affected Entities	If the user has a filter preventing him or her from viewing all of the individual entities attached to an entity group, he or she will see the following message at the top of th • You are not able to see all the entities on this page because you are restricted from seeing [number of hidden entities] entities.
Tickets	Displays tickets associated with a specific vulnerability.
Technologies	Lists the technologies associated with the vulnerability. Use this tab to create and manage technologies. **NOTE**: By default the property in the **Agiliance.Properties** file that displays Technologies in this tab reads as `cpe.uri.regexp.criteria =version:rightMatch::update_:rightMatch::edition:equalsMatch::language:equalsMatch::software_edition:equalsMatch::target_software:equalsMatch::target_` which shows technologies as per wild card match. To change the criteria of the displayed technologies in the **Technologies** tab, users can change the operator of the desi **anyMatch** in the above property.
Patches	Once vulnerabilities have been disseminated to vulnerability administrators, the vulnerability instances are fixed with a patch, usually provided by the vendor. Connecto Connector can provide information about available patches.
Exceptions	Shows exceptions associated with a specific vulnerability. Users can also create new exceptions and add them to the vulnerability.
Threats	Lists the threats associated with this vulnerability.