

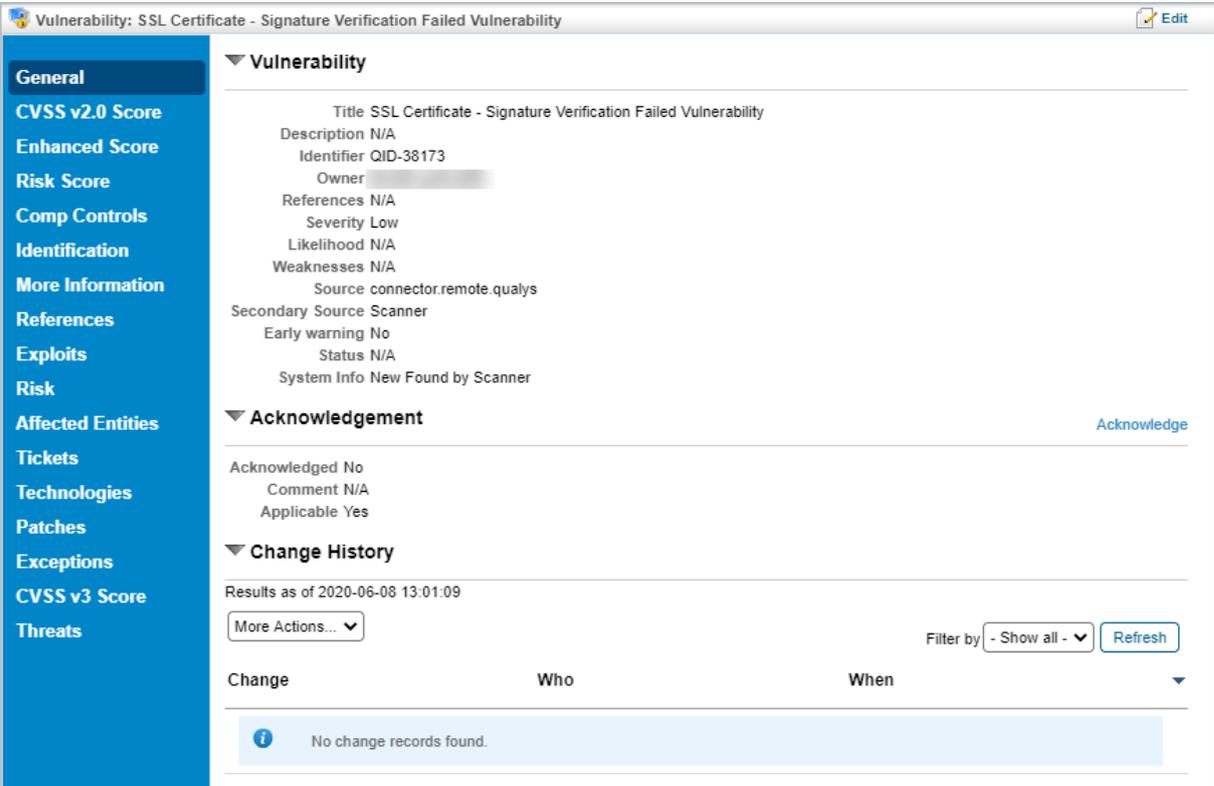
Add Exceptions to Vulnerabilities

You can create or add an existing exception manually to establish a single link between a vulnerability and an entity group or a one-to-one link between a vulnerability and an entity. An exception that is linked to a vulnerability will help you track the affected entities and mitigation procedures to fix a vulnerability.

Existing exceptions can only be added through a vulnerability's **Affected Entities** tab, while new exceptions can also be created in the **Exceptions** tab. To create an exception manually, you must have the Exception View, Request, and Threats and Vulnerabilities View permissions. Adding an existing ticket or exception to a vulnerability requires the View and Request permissions.

To create an exception in Affected Entities:

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



The screenshot shows a web interface for a vulnerability. The title bar reads "Vulnerability: SSL Certificate - Signature Verification Failed Vulnerability" with an "Edit" button. A blue sidebar on the left contains navigation tabs: General (selected), CVSS v2.0 Score, Enhanced Score, Risk Score, Comp Controls, Identification, More Information, References, Exploits, Risk, Affected Entities, Tickets, Technologies, Patches, Exceptions, CVSS v3 Score, and Threats. The main content area is divided into sections: "Vulnerability" with fields for Title, Description, Identifier, Owner, References, Severity, Likelihood, Weaknesses, Source, Secondary Source, Early warning, Status, and System Info; "Acknowledgement" with fields for Acknowledged, Comment, and Applicable; and "Change History" with a "Results as of" timestamp, a "More Actions..." dropdown, a "Filter by" dropdown set to "Show all", and a "Refresh" button. Below the change history is a table with columns "Change", "Who", and "When", which is currently empty and displays a message: "No change records found."

The Vulnerability details page.

4. Click the **Affected Entities** tab.

Vulnerability: SSL Certificate - Signature Verification Failed Vulnerability

Vulnerable entity groups

The following entity groups have a technology affected by this vulnerability.

1-6 of 6

Filter by:

<input type="checkbox"/>	OS Name	OS Vendor	OS Version	Owner	Criticality	Risk Score	Total Affected	Scanner Reported	Without Ticket	Without Ticket and Exception	Patch Installed
<input type="checkbox"/>	advanced_core_operating_system	a10networks	2.7.1			30	1	0	0	0	0
<input type="checkbox"/>	N/A	N/A	N/A			9	2	0	0	0	0
<input type="checkbox"/>	N/A	N/A	N/A			21	4	0	0	0	0
<input type="checkbox"/>	N/A	N/A	N/A			30	1	0	0	0	0
<input type="checkbox"/>	N/A	N/A	N/A	N/A		21	1	1	0	0	0
<input type="checkbox"/>	N/A	N/A	N/A			30	2	0	0	0	0

The Affected Entities tab.

5. Perform any one of the following actions:

- To create a new exception:
 - Select an entity group and click **Create Exception** to create a single exception for all affected entities in that group. You can also select multiple entity groups to create a single exception.
- To create individual exception for each entity in a group:
 - Click **View Entities** in the entity group that has more than one entity, select an entity, and then click **Create Exception**.
- To add an existing exception
 - Select an entity group, then click **Add to existing Exception**. Select an exception, then click **OK**. You can also select multiple entity groups to add an existing exception.
 - For entities in a group, click **View Entities** in the entity group row that has more than one affected entity. Select an entity, then click **Add to existing Exception**. Select a ticket, then click **OK**.

To create an exception in Exceptions:

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

Vulnerability: SSL Certificate - Signature Verification Failed Vulnerability Edit

General

CVSS v2.0 Score
Enhanced Score
Risk Score
Comp Controls
Identification
More Information
References
Exploits
Risk
Affected Entities
Tickets
Technologies
Patches
Exceptions
CVSS v3 Score
Threats

Vulnerability

Title SSL Certificate - Signature Verification Failed Vulnerability
Description N/A
Identifier QID-38173
Owner [Redacted]
References N/A
Severity Low
Likelihood N/A
Weaknesses N/A
Source connector.remote.qualys
Secondary Source Scanner
Early warning No
Status N/A
System Info New Found by Scanner

Acknowledgement Acknowledge

Acknowledged No
Comment N/A
Applicable Yes

Change History

Results as of 2020-06-08 13:01:09
More Actions... Filter by - Show all - Refresh

Change	Who	When
No change records found.		

The Vulnerability details page.

- Click the **Exceptions** tab.

Vulnerability: SSL Certificate - Signature Verification Failed Vulnerability

Exceptions

1-1 of 1
New More Actions... Filter by - Show all - Refresh

Exception ID	Exception Name	Global Entity Names	Current Stage	Status	Status Modified By	Requestor	Start	End	Total Entities
EXP00218	entity	✓ qa103,qa100,qa102,qa101	Sign Off	Approve1	[Redacted]	[Redacted]	2020-04-15	N/A	4

Exceptions

The Exceptions tab.

- Click **New** to create a single exception that will use the selected vulnerability as its vulnerability scope and definition.

Exception Request
✕

1. Basic Details

2. Attach File

Step 1: Enter Exception Request Information

* = required

Title*

Vulnerability Scope Vulnerability Definition(s)

Vulnerability Definition(s) [SSL Certificate - Signature Verification Failed Vulnerability](#)

Entities Scope*

Reason for Exception

Start Date

End Date

Next Review Date

Cancel
< Back
Next >
Finish

The Exception Request wizard.

Users creating an exception from the **Exceptions** tab will not be able to modify the vulnerability scope.

For more information on creating a new exception, see [Create an Exception Request](#). For information on creating an exception from a ticket object, see [Create a Vulnerability Exception on a Ticket](#)