ThreatQuotient

Qualys Scanner CDF User Guide

Version 1.0.0

August 22, 2023

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support
Email: support@threatq.com
Web: support.threatq.com
Phone: 703.574.9893

Contents

Warning and Disclaimer

ThreatQuotient, Inc. provides this document “as is”, without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein. ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information.

Support

This integration is designated as **ThreatQ Supported**.

Support Email: support@threatq.com
Support Web: https://support.threatq.com
Support Phone: 703.574.9893

Integrations/apps/add-ons designated as **ThreatQ Supported** are fully supported by ThreatQuotient's Customer Support team.

ThreatQuotient strives to ensure all ThreatQ Supported integrations will work with the current version of ThreatQuotient software at the time of initial publishing. This applies for both Hosted instance and Non-Hosted instance customers.

> ThreatQuotient does not provide support or maintenance for integrations, apps, or add-ons published by any party other than ThreatQuotient, including third-party developers.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.0.0
Compatible with ThreatQ Versions	>= 5.10.0
Support Tier	ThreatQ Supported

Introduction

The Qualys Scanner CDF collects information about Qualys scans executed in the past user-set days, including all CVEs related to those vulnerabilities, and ingests them into the ThreatQ platform.

The integration provides the following feeds:

- **Qualys Scanner** - ingests vulnerabilities, indicators and assets from Qualys scans
- **Qualys Unrelate Patched QIDs (supplemental)** - unrelates patched vulnerabilities and indicators of type CVE from assets
- **Qualys Get TQObjects (supplemental)** - retrieves objects from ThreatQ Threat Library.
- **Qualys Scanner CVE Knowledge Base (supplemental)** - queries the Qualys database to obtain more information about a vulnerability
- **Qualys Scanner Query QIDs (supplemental)** - submits vulnerabilities batches identified by QID (Qualys ID) to `Qualys Scanner CVE Knowledge Base` feed

The integration ingests the following system objects:

- Assets
- Indicators
- Vulnerabilities

Installation

Perform the following steps to install the integration:

> The same steps can be used to upgrade the integration to a new version.

1. Log into https://marketplace.threatq.com/.
2. Locate and download the integration file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration file using one of the following methods:
   - Drag and drop the file into the dialog box
   - Select **Click to Browse** to locate the integration file on your local machine

   > ThreatQ will inform you if the feed already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the feed contains changes to the user configuration. The new user configurations will overwrite the existing ones for the feed and will require user confirmation before proceeding.

6. If prompted, select the individual feeds to install and click **Install**. The feed will be added to the integrations page.

You will still need to configure and then enable the feed.

Configuration

> ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

To configure the integration:

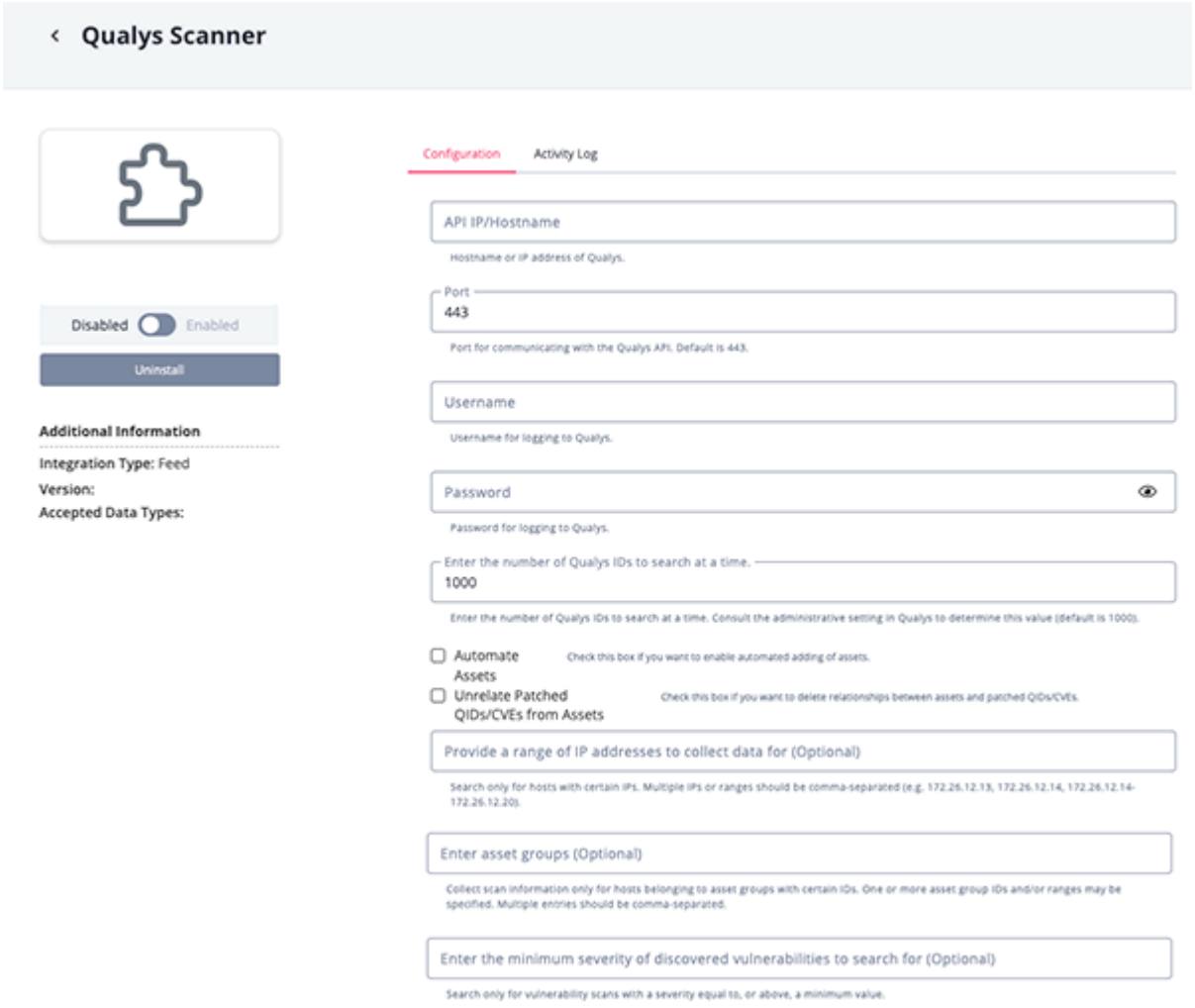
1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** option from the *Category* dropdown (optional).

   > If you are installing the integration for the first time, it will be located under the **Disabled** tab.

3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
API IP/Hostname	The Hostname or IP address of Qualys.
Port	The port for communicating with the Qualys API. The default setting is **443**.
Username	Your Qualys username.
Password	The password associated with the username above.
Enter the Number of Qualys IDs to Search at a Time	Enter the number of Qualys IDs to search at a time. Consult the administrative setting in Qualys to determine this value. The default value is **1000**.
Automate Assets	Select this option to enable automated adding of assets.
Unrelate Patched QIDs/CVEs from Assets	Select this option to delete relationships between assets and patched QIDs/CVEs.
Provide a Range of IP Addresses to Collect Data for	Optional - Search only for hosts with certain IPs. Multiple IPs or ranges should be comma-separated (e.g. 172.26.12.13, 172.26.12.14, 172.26.12.14-172.26.12.20).

PARAMETER	DESCRIPTION
Enter Asset Groups	Optional - Collect scan information only for hosts belonging to asset groups with certain IDs. One or more asset group IDs and/or ranges may be specified. Multiple entries should be comma-separated.
Enter the Minimum Severity of Discovered Vulnerabilities in Search for	Optional - Search only for vulnerability scans with a severity equal to, or above, a minimum value.



5. Review any additional settings, make any changes if needed, and click on **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable it.

ThreatQ Mapping

Qualys Scanner

The Qualys Scanner feed ingests vulnerabilities, indicators and assets from Qualys scans.

`GET https://{HOSTNAME}:{PORT}/api/2.0/fo/asset/host/vm/detection/`

Sample Request Parameters:

```
{
    "action": "list"
    "show_results": 1,
    "output_format": "XML",
    "show_igs": 1,
    "status": "New,Active,Re-Opened,Fixed",
    "vm_scan_date_after": "2023-07-13T11:51:00Z",
    "severities": "2"
}
```

Truncated Sample Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_VM_DETECTION_OUTPUT SYSTEM
        "https://qualysapi.qg2.apps.qualys.com/api/2.0/fo/asset/host/vm/
detection/dtd/output.dtd">
<!-- This report was generated with an evaluation version of  //-->
<HOST_LIST_VM_DETECTION_OUTPUT>
    <RESPONSE>
        <DATETIME>2023-07-13T13:15:11Z</DATETIME>
        <!-- keep-alive for HOST_LIST_VM_DETECTION_OUTPUT  -->
        <HOST_LIST>
            <HOST>
                <ID>503005297</ID>
                <IP>172.16.114.111</IP>
                <DNS>
                    <![CDATA[ec2-18-233-226-119.compute-1.amazonaws.com]]>
                </DNS>
                <TRACKING_METHOD>IP</TRACKING_METHOD>
                <LAST_SCAN_DATETIME>2023-07-13T11:53:02Z</LAST_SCAN_DATETIME>
                <LAST_VM_SCANNED_DATE>2023-07-13T11:51:32Z</
LAST_VM_SCANNED_DATE>
                <LAST_VM_SCANNED_DURATION>7919</LAST_VM_SCANNED_DURATION>
                <DETECTION_LIST>
                    <DETECTION>
                        <QID>6</QID>
                        <TYPE>Info</TYPE>
                        <SEVERITY>1</SEVERITY>
                        <RESULTS>
```

```
                            <![CDATA[IP address       Host name 172.16.114.111
No registered hostname]]>
                        </RESULTS>
                        <FIRST_FOUND_DATETIME>2023-07-13T10:59:28Z</
FIRST_FOUND_DATETIME>
                        <LAST_FOUND_DATETIME>2023-07-13T11:51:32Z</
LAST_FOUND_DATETIME>
                        <TIMES_FOUND>2</TIMES_FOUND>
                        <IS_DISABLED>0</IS_DISABLED>
                        <LAST_PROCESSED_DATETIME>2023-07-13T11:53:02Z</
LAST_PROCESSED_DATETIME>
                    </DETECTION>
                </DETECTION_LIST>
            </HOST>
        </HOST_LIST>
    </RESPONSE>
</HOST_LIST_VM_DETECTION_OUTPUT>
        <!-- This report was generated with an evaluation version of  //-->
        <!-- CONFIDENTIAL AND PROPRIETARY INFORMATION. Qualys provides the
QualysGuard Service "As Is," without any warranty of any kind. Qualys makes no
warranty that the information contained in this report is complete or error-
free. Copyright 2023, Qualys, Inc. //-->
```

Assets are ingested only is user configuration Automate Assets is checked.

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
HOST_LIST_VM_DETECTION_ OUTPUT.RESPONSE.HOST_LIST.HOST[].IP	Asset Value	N/A	N/A	172.16.114.111	N/A
HOST_LIST_VM_DETECTION_ OUTPUT.RESPONSE.HOST_LIST.HOST[].ID	Asset Attribute	Host ID	N/A	503005297	N/A
HOST_LIST_VM_DETECTION_ OUTPUT.RESPONSE.HOST_LIST.HOST[]. TRACKING_METHOD	Asset Attribute	Tracking Method	N/A	IP	N/A
HOST_LIST_VM_DETECTION_OUTPUT. RESPONSE.HOST_LIST.HOST[].DNS	Asset Attribute	DNS Hostname	N/A	ec2-18-233-226-119.compute-1. amazonaws.com	N/A

The values from `HOST_LIST_VM_DETECTION_OUTPUT.RESPONSE.HOST_LIST.HOST[].DETECTION_LIST.DETECTION[].QID` will be sent to the feed `Qualys Scanner Query QIDs` to bring information about the vulnerability associated with this Qualys ID (QID) if the following conditions are true:

- `HOST_LIST_VM_DETECTION_OUTPUT.RESPONSE.HOST_LIST.HOST[].DETECTION_LIST.DETECTION[].STATUS` does not exist or its value is different from `Fixed`
- `HOST_LIST_VM_DETECTION_OUTPUT.RESPONSE.HOST_LIST.HOST[].DETECTION_LIST.DETECTION[].STATUS` exists and has the value `Fixed` but more recent data is not fixed

The values from `HOST_LIST_VM_DETECTION_OUTPUT.RESPONSE.HOST_LIST.HOST[].DETECTION_LIST.DETECTION[].QID` will be sent to the feed `Qualys Unrelate Patched QIDs` if `HOST_LIST_VM_DETECTION_OUTPUT.RESPONSE.HOST_LIST.HOST[].DETECTION_LIST.DETECTION[].STATUS` exists and has the value `Fixed` and also there is no recent data that is not fixed.

Qualys Unrelate Patched QIDs (Supplemental)

The Qualys Unrelate Patched QIDs supplemental feed receives a list of QIDs of fixed vulnerabilities, and it uses the API filter from Pynoceros to unrelate them from assets.

1. First, the feed will call the `Qualys Get TQObjects` supplemental feed to get a list of assets from ThreatQ Library.
2. The feed will then iterate over the assets extracted from ThreatQ Library and delete the relationships with the list of received fixed vulnerabilities and their associated indicators.

`DELETE https://{THREATQ_HOSTNAME}/asset/{ASSET_ID}/vulnerability/{FIXED_VULN_PIVOT_ID}` `DELETE https://{THREATQ_HOSTNAME}/asset/{ASSET_ID}/indicators/{FIXED_VULN_RELATED_INDICATOR_PIVOT_ID}`

> The feed is executed only if the user configuration `Unrelate Patched QIDs/CVEs from Assets` is enabled.

Qualys Get TQObjects (Supplemental)

The Qualys Get TQObjects supplemental feed uses the API filter from Pynoceros to get all the existing assets from ThreatQ Library for which at least one of the sources is `Qualys Scanner`.

`GET https://{THREATQ_HOSTNAME}/asset`

Sample API Request:

```
{
    "sources.name": "Qualys Scanner"
    "withp": "indicators,vulnerability,vulnerability.attributes,vulnerability.indicators"
}
```

Qualys Scanner CVE Knowledge Base (Supplemental)

The Qualys Scanner CVE Knowledge Base supplemental feed queries Qualys database to obtain more information about a vulnerability.

```
GET https://{HOSTNAME}:{PORT}/api/2.0/fo/knowledge_base/vuln/
```

Sample API Request:

```
{
    "action": "list"
    "details": "Basic",
    "ids": "38173"
}
```

Truncated Sample Request:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE KNOWLEDGE_BASE_VULN_LIST_OUTPUT SYSTEM
        "https://qualysapi.qg2.apps.qualys.com/api/2.0/fo/knowledge_base/vuln/
knowledge_base_vuln_list_output.dtd">
<!-- This report was generated with an evaluation version of  //-->
<KNOWLEDGE_BASE_VULN_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2023-08-17T07:36:41Z</DATETIME>
        <VULN_LIST>
            <VULN>
                <QID>38173</QID>
                <VULN_TYPE>Vulnerability or Potential Vulnerability</VULN_TYPE>
                <SEVERITY_LEVEL>2</SEVERITY_LEVEL>
                <TITLE>
                    <![CDATA[SSL Certificate - Signature Verification Failed
Vulnerability]]>
                </TITLE>
                <CATEGORY>General remote services</CATEGORY>
                <LAST_SERVICE_MODIFICATION_DATETIME>2022-02-28T13:28:19Z</
LAST_SERVICE_MODIFICATION_DATETIME>
                <PUBLISHED_DATETIME>2003-01-29T20:37:41Z</PUBLISHED_DATETIME>
                <PATCHABLE>0</PATCHABLE>
                <SOFTWARE_LIST>
                    <SOFTWARE>
                        <PRODUCT>
                            <![CDATA[dns_server]]>
                        </PRODUCT>
                        <VENDOR>
                            <![CDATA[multi-vendor]]>
                        </VENDOR>
                    </SOFTWARE>
                </SOFTWARE_LIST>
                <VENDOR_REFERENCE_LIST>
                    <VENDOR_REFERENCE>
```

```
                        <ID>
                            <![CDATA[Joomla! Security]]>
                        </ID>
                        <URL>
                            <![CDATA[https://developer.joomla.org/security-
centre/894-20230201-core-improper-access-check-in-webservice-endpoints.html]]>
                        </URL>
                    </VENDOR_REFERENCE>
                </VENDOR_REFERENCE_LIST>
                <CVE_LIST>
                    <CVE>
                        <ID>
                            <![CDATA[CVE-2023-23752]]>
                        </ID>
                        <URL>
                            <![CDATA[http://cve.mitre.org/cgi-bin/cvename.cgi?
name=CVE-2023-23752]]>
                        </URL>
                    </CVE>
                </CVE_LIST>
                <DIAGNOSIS>
                    <![CDATA[An SSL Certificate associates an entity (person,
organization, host, etc.) with a Public Key. ]]>
                </DIAGNOSIS>
                <CONSEQUENCE>
                    <![CDATA[By exploiting this vulnerability, man-in-the-
middle attacks in tandem with DNS cache poisoning can occur.]]>
                </CONSEQUENCE>
                <SOLUTION>
                    <![CDATA[Please install a server certificate signed by a
trusted third-party Certificate Authority.]]>
                </SOLUTION>
                <PCI_FLAG>1</PCI_FLAG>
                <THREAT_INTELLIGENCE>
                    <THREAT_INTEL id="5">
                        <![CDATA[Easy_Exploit]]>
                    </THREAT_INTEL>
                    <THREAT_INTEL id="8">
                        <![CDATA[No_Patch]]>
                    </THREAT_INTEL>
                </THREAT_INTELLIGENCE>
                <DISCOVERY>
                    <REMOTE>1</REMOTE>
                </DISCOVERY>
            </VULN>
        </VULN_LIST>
    </RESPONSE>
</KNOWLEDGE_BASE_VULN_LIST_OUTPUT>
        <!-- This report was generated with an evaluation version of  //-->
        <!-- CONFIDENTIAL AND PROPRIETARY INFORMATION. Qualys provides the
```

```
QualysGuard Service "As Is," without any warranty of any kind. Qualys makes no
warranty that the information contained in this report is complete or error-
free. Copyright 2023, Qualys, Inc. //-->
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN[].TITLE	Related Vulnerability Value	N/A	KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.PUBLISHED_DATETIME	Certificate - Signature Verification Failed Vulnerability	N/A
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN[].DIAGNOSIS	Related Vulnerability Description	N/A	N/A	An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key.	N/A
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN[].QID	Related Vulnerability Attribute	Qualys Id	KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.PUBLISHED_DATETIME	38173	N/A
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN[].VULN_TYPE	Related Vulnerability Attribute	Vulnerability Type	KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.PUBLISHED_DATETIME	Vulnerability or Potential Vulnerability	N/A
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN[].SEVERITY_LEVEL	Related Vulnerability Attribute	Severity	KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.PUBLISHED_DATETIME	2	If the attribute already exists, the value will be updated.
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN[].CATEGORY	Related Vulnerability Attribute	Category	KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.PUBLISHED_DATETIME	General remote services	N/A
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN[].PATCHABLE	Related Vulnerability Attribute	Patchable	KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.PUBLISHED_DATETIME	NO	Mapped to YES/NO. If the attribute already exists, the value will be updated.
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN[].PCI_FLAG	Related Vulnerability Attribute	PCI Flag	KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.PUBLISHED_DATETIME	1	N/A
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN[].LAST_SERVICE_MODIFICATION_DATETIME	Related Vulnerability Attribute	Last Server Modification Time	KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.PUBLISHED_DATETIME	2022-02-28T13:28:19Z	If the attribute already exists, the value will be updated.
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN[].SOFTWARE_LIST.SOFTWARE[].PRODUCT	Related Vulnerability Attribute	Product	KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.PUBLISHED_DATETIME	dns_server	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN[].SOFTWARE_LIST.SOFTWARE[].VENDOR	Related Vulnerability Attribute	Vendor	KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.PUBLISHED_DATETIME	multi-vendor	N/A
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN[].VENDOR_REFERENCE_LIST.VENDOR_REFERENCE.ID	Related Vulnerability Attribute	Vendor Reference Id	KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.PUBLISHED_DATETIME	Joomla! Security	N/A
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN[].VENDOR_REFERENCE_LIST.VENDOR_REFERENCE.URL	Related Vulnerability Attribute	Vendor Reference URL	KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.PUBLISHED_DATETIME	https://developer.joomla.org/security-centre/894-20230201-core-improper-access-check-in-webservice-endpoints.html	N/A
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN[].CVSS.BASE	Related Vulnerability Attribute	CVSS Score	KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.PUBLISHED_DATETIME	N/A	If the attribute already exists, the value will be updated.
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN[].CVSS.TEMPORAL	Related Vulnerability Attribute	CVSS Temporal	KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.PUBLISHED_DATETIME	N/A	If the attribute already exists, the value will be updated.
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN[].CVSS.ACCESS.VECTOR	Related Vulnerability Attribute	Access Vector	KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.PUBLISHED_DATETIME	N/A	N/A
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN[].CVSS.ACCESS.COMPLEXITY	Related Vulnerability Attribute	Access Complexity	KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.PUBLISHED_DATETIME	N/A	N/A
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN[].CVSS.IMPACT.CONFIDENTIALITY	Related Vulnerability Attribute	Confidentiality Impact	KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.PUBLISHED_DATETIME	N/A	N/A
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN[].CVSS.IMPACT.INTEGRITY	Related Vulnerability Attribute	Integrity Impact	KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.PUBLISHED_DATETIME	N/A	N/A
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN[].CVSS.IMPACT.AVAILABILITY	Related Vulnerability Attribute	Availability Impact	KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.PUBLISHED_DATETIME	N/A	N/A
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN[].CVSS.AUTHENTICATION	Related Vulnerability Attribute	Authentication	KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.PUBLISHED_DATETIME	N/A	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN[].CVSS.EXPLOITABILITY	Related Vulnerability Attribute	Exploitability	KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.PUBLISHED_DATETIME	N/A	N/A
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN[].CVSS.REMEDIATION_LEVEL	Related Vulnerability Attribute	Remediation Level	KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.PUBLISHED_DATETIME	N/A	N/A
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN[].CVSS.REPORT_CONFIDENCE	Related Vulnerability Attribute	Report Confidence	KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN.PUBLISHED_DATETIME	N/A	N/A
KNOWLEDGE_BASE_VULN_LIST_OUTPUT.RESPONSE.VULN_LIST.VULN[].CVE_LIST.CVE[].ID	Related Indicator Value	CVE	N/A	CVE-2023-23752	N/A
N/A	Related Indicator Attribute	Vulnerability found by Qualys	N/A	Yes	N/A

Qualys Scanner Query QIDs (Supplemental)

The Qualys Scanner Query QIDs supplemental feed receives a list of QIDs from `Qualys Scanner` that should be enriched. The feed splits them into batches according to the user configuration `Enter the number of Qualys IDs to search at a time` and sends them to `Qualys Scanner CVE Knowledge Base` feed.

Average Feed Run

> Object counts and Feed runtime are supplied as generalities only - objects returned by a provider can differ based on credential configurations and Feed runtime may vary based on system resources and load.

Qualys Scanner

METRIC	RESULT
Run Time	1 min
Assets	31
Asset Attributes	64
Indicators	90
Indicator Attributes	90
Vulnerabilities	129
Vulnerability Attributes	1,286

Change Log

- **Version 1.0.0**
  - Initial release