ThreatQuotient

CISA Known Exploited Vulnerabilities CDF Guide

Version 1.0.0

April 25, 2022

ThreatQuotient
11400 Commerce Park Dr., Suite 200
Reston, VA 20191

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.

Versioning

- Current integration version: `1.0.0`
- Compatible with ThreatQ versions >= `4.35.0`

Introduction

The Cybersecurity and Infrastructure Security Agency (CISA) is a United States federal agency, an operational component under Department of Homeland Security (DHS) oversight. Its activities are a continuation of the National Protection and Programs Directorate (NPPD).

CISA Known Exploited Vulnerabilities CDF consists of one feed:

- **CISA Known Exploited Vulnerabilities** - ingests Vulnerabilities and Indicators as well as their attributes.

CISA Known Exploited Vulnerabilities CDF ingests the following object types:

- Vulnerabilities
  - Vulnerability Attributes
- Indicators
  - Indicators Attributes

Installation Guide

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.

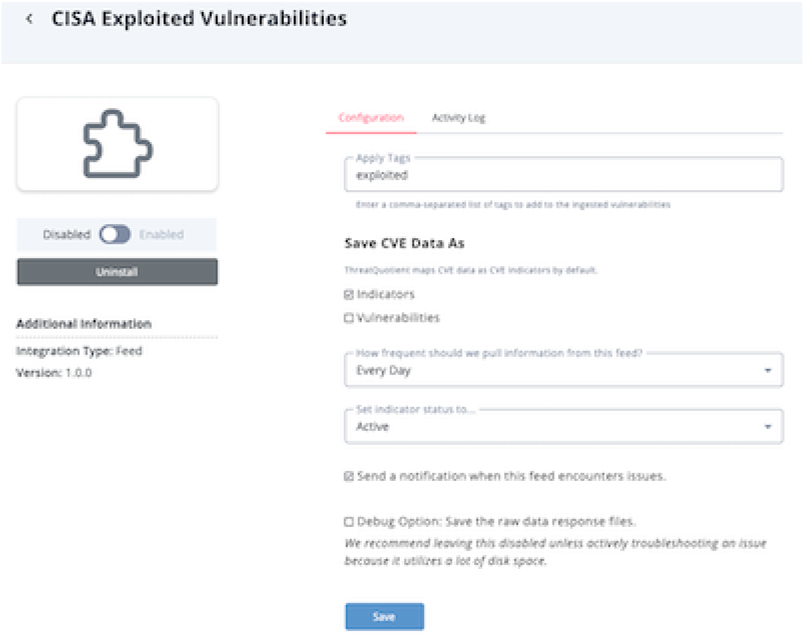
To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **OSINT** 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 to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Apply Tags	List of tags to add to the ingested vulnerabilities.
Save CVE Data As	Select whether to ingest CVEs as ThreatQ Vulnerability objects, Indicator objects, or both. Defaults to ingesting only Indicator objects. • Indicators • Vulnerabilities



Additional Information

Integration Type: Feed

Version: 1.0.0

Apply Tags: exploited

Enter a comma-separated list of tags to add to the ingested vulnerabilities

Save CVE Data As

ThreatQuotient maps CVE data as CVE indicators by default.

☑ Indicators

□ Vulnerabilities

How frequent should we pull information from this feed?: Every Day

Set indicator status to...: Active

☑ Send a notification when this feed encounters issues.

□ Debug Option: Save the raw data response files.

We recommend leaving this disabled unless actively troubleshooting an issue because it utilizes a lot of disk space.

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

CISA Known Exploited Vulnerabilities

The CISA Known Exploited Vulnerabilities feed ingests Vulnerabilities and Indicators as well as their attributes.

```
GET https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json
```

Sample Response:

```
{
   {
  "title": "CISA Catalog of Known Exploited Vulnerabilities",
  "catalogVersion": "2022.04.06",
  "dateReleased": "2022-04-06T14:23:03.033Z",
  "count": 616,
  "vulnerabilities": [
    {
      "cveID": "CVE-2021-27104",
      "vendorProject": "Accellion",
      "product": "FTA",
      "vulnerabilityName": "Accellion FTA OS Command Injection Vulnerability",
      "dateAdded": "2021-11-03",
      "shortDescription": "Accellion FTA 9_12_370 and earlier is affected by OS command execution via a crafted POST
request to various admin endpoints.",
      "requiredAction": "Apply updates per vendor instructions.",
      "dueDate": "2021-11-17"
    },
    {
      "cveID": "CVE-2021-27102",
      "vendorProject": "Accellion",
      "product": "FTA",
      "vulnerabilityName": "Accellion FTA OS Command Injection Vulnerability",
      "dateAdded": "2021-11-03",
      "shortDescription": "Accellion FTA 9_12_411 and earlier is affected by OS command execution via a local web
service call.",
      "requiredAction": "Apply updates per vendor instructions.",
      "dueDate": "2021-11-17"
    }
  ]
}
```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data[].cveID	Related Vulnerability.Value/ Related Indicator.Value	N/A/ CVE	.data[].dateAdded	CVE-2021-27104	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data[].vendorProject	Vulnerability.Attribute/ Indicator.Attribute	Affected Vendor	.data[].dateAdded	Accellion	N/A
.data[].shortDescription	Vulnerability.Attribute/ Indicator.Attribute	Description	.data[].dateAdded	Accellion FTA 9_12_370 and earlier is(...)	N/A
.data[].product	Vulnerability.Attribute/ Indicator.Attribute	Affected Product	.data[].dateAdded	FTA	N/A
.data[].requiredAction	Vulnerability.Attribute/ Indicator.Attribute	Action Required	.data[].dateAdded	Apply updates per vendor instructions.	N/A
.data[].vulnerabilityName	Vulnerability.Attribute/ Indicator.Attribute	Vulnerability Name	.data[].dateAdded	Accellion FTA OS Command Injection Vulnerability	N/A

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.

CISA Known Exploited Vulnerabilities

METRIC	RESULT
Run Time	2 minutes
Vulnerabilities	616
Vulnerability Attributes	2,457
Indicators	616
Indicators Attributes	2,457

Change Log

- **Version 1.0.0**
    - Initial release