ThreatQuotient

National Vulnerability Database (NVD) CVE CDF Guide

Version 3.0.3

June 13, 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	3.0.3
Compatible with ThreatQ Versions	>= 4.27.0
Support Tier	ThreatQ Supported

Introduction

The National Vulnerability Database (NVD) CVE feed consumes information published by NIST about vulnerabilities. Historic data is provided in a specific package for that year and any new data, updates, or corrections defined from the previous eight days are provided in the "modified" package. Currently, historic records are available for all years between 2002 and present time.

The integration provides the following feed:

- **NVD CVE** - ingests information about vulnerabilities.

The integration ingests the following system objects:

- Indicators
  - Indicator Attributes
- Vulnerabilities
  - Vulnerability Attributes

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:

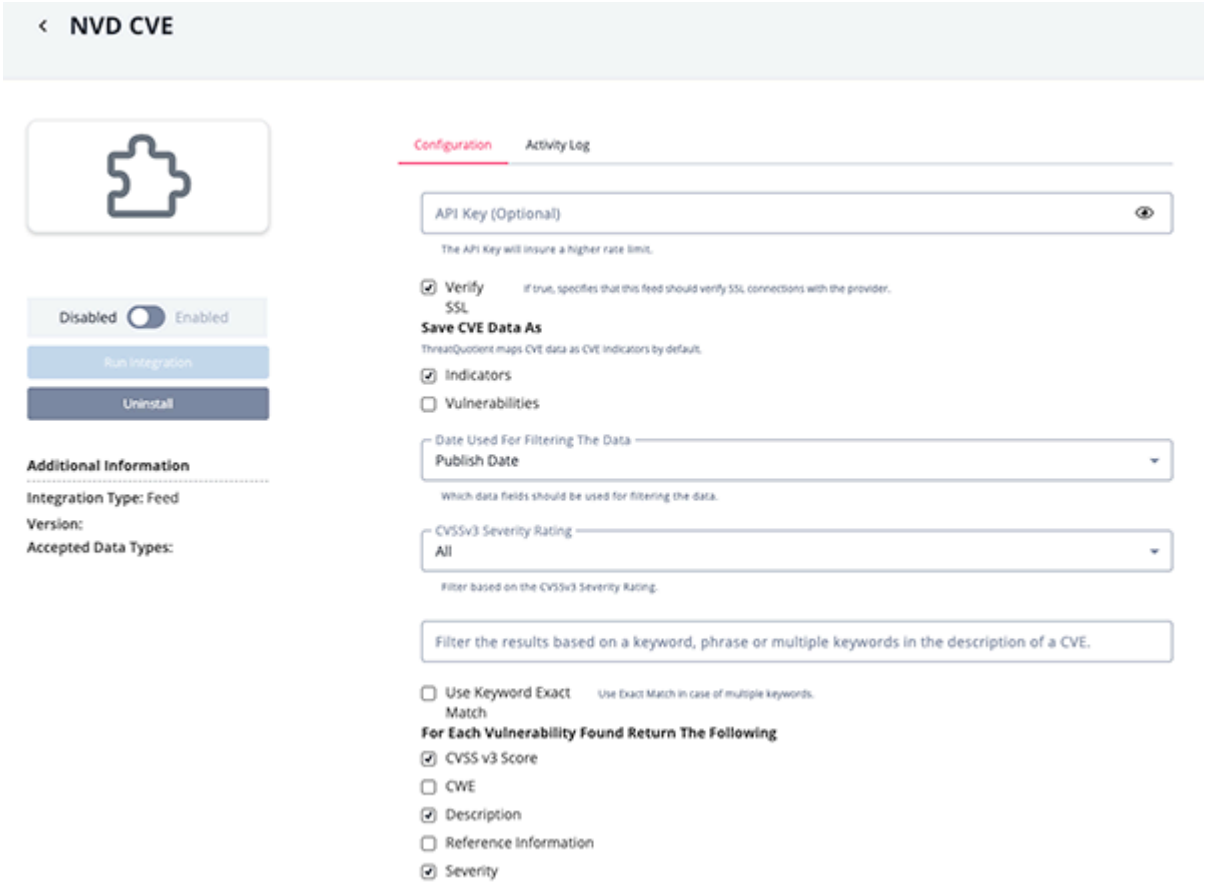
1. Navigate to your integrations management page in ThreatQ.
2. Select the **OSINT** option from the *Category* dropdown (optional).

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

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

PARAMETER	DESCRIPTION
API Key	Optional - Enter your NVD API Key to allow higher rate limits.
Save CVE Data as	This parameter is required and can be configured to have the feed ingest CVE data such as indicators, vulnerabilities, or both.
Verify SSL Certificate	Whether to verify the server's SSL Certificate.
Date used for Filtering the Data	Select which data fields should be used for filtering the data. Options include **Publish Date** (default) and **Modified Date**.
CVSSv3 Severity Rating	Filter the data based on the CVSSv3 Severity Rating. Options include: ◦ All (default) ◦ Low

PARAMETER	DESCRIPTION
	◦ Medium ◦ High ◦ Critical
Filter the results based on a keyword, phrase or multiple keywords in the description of a CVE	Enter keyword(s) to be used to filter the results.
Use Keyword Exact Match	Enable this option in the event of using multiple keywords in the parameter above.
For Each Vulnerability Found Return the Following	Select the data that will be returned with each vulnerability. Options include:



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

NVD CVE

Scheduled runs ingest CVE data from the "modified" package. Manual runs will request the package for the year specified by the `Start Date` parameter. When triggering a manual run, only the year field of the `Start Date` is evaluated. If a `Start Date` prior to 2002 is selected for a manual feed run, the 2002 package will be requested.

Ingested CVE data can be mapped as CVE Indicators (default configuration), Vulnerabilities, or both.

`GET https://services.nvd.nist.gov/rest/json/cves/2.0`

Sample Response:


```
{
  "resultsPerPage": 10,
  "startIndex": 0,
  "totalResults": 10,
  "format": "NVD_CVE",
  "version": "2.0",
  "timestamp": "2023-04-07T08:55:08.963",
  "vulnerabilities": [
    {
      "cve": {
        "id": "CVE-2022-41696",
        "sourceIdentifier": "ics-cert@hq.dhs.gov",
        "published": "2023-03-21T23:15:12.167",
        "lastModified": "2023-03-23T16:11:41.357",
        "vulnStatus": "Analyzed",
        "descriptions": [
          {
            "lang": "en",
            "value": "Versions of VISAM VBASE Automation Base prior to 11.7.5 may disclose information if a valid
user opens a specially crafted file."
          }
        ],
        "metrics": {
          "cvssMetricV31": [
            {
              "source": "nvd@nist.gov",
              "type": "Primary",
              "cvssData": {
                "version": "3.1",
                "vectorString": "CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N",
                "attackVector": "LOCAL",
                "attackComplexity": "LOW",
                "privilegesRequired": "NONE",
```

```
              "userInteraction": "REQUIRED",
              "scope": "UNCHANGED",
              "confidentialityImpact": "HIGH",
              "integrityImpact": "NONE",
              "availabilityImpact": "NONE",
              "baseScore": 5.5,
              "baseSeverity": "MEDIUM"
            },
            "exploitabilityScore": 1.8,
            "impactScore": 3.6
          }
        ]
      },
      "weaknesses": [
        {
          "source": "ics-cert@hq.dhs.gov",
          "type": "Primary",
          "description": [
            {
              "lang": "en",
              "value": "CWE-611"
            }
          ]
        }
      ],
      "configurations": [
        {
          "nodes": [
            {
              "operator": "OR",
              "negate": false,
              "cpeMatch": [
                {
                  "vulnerable": true,
                  "criteria": "cpe:2.3:a:visam:vbase_automation_base:*:*:*:*:*:*:*:*",
                  "versionEndExcluding": "11.7.5",
                  "matchCriteriaId": "DE95E148-09BB-49BC-9DF5-633BAED35181"
                }
              ]
            }
          ]
        }
      ],
      "references": [
        {
          "url": "https://www.cisa.gov/news-events/ics-advisories/icsa-23-080-05",
          "source": "ics-cert@hq.dhs.gov",
          "tags": [
            "Third Party Advisory",
            "US Government Resource"
          ]
        }
      ]
    }
  }
 ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.vulnerabilities[].cve.id	Indicator.Value / Vulnerability.Value	CVE / `N/A`	.vulnerabilities[].cve.published	CVE-2018-6363	N/A
.vulnerabilities[].cve.descriptions[].value	Indicator.Description / Vulnerability.Description	`N/A`	.vulnerabilities[].cve.published	SQL Injection exists in Task Rabbit Clone 1.0 via the single_blog.php id parameter.	If `Description` option is selected
.vulnerabilities[].cve.lastModified	Indicator.Attribute / Vulnerability.Attribute	Last Modified	.vulnerabilities[].cve.published	2023-03-24T20:34:11.990	If the attribute already exists, the value will be updated.
.vulnerabilities[].cve.id	Indicator.Attribute / Vulnerability.Attribute	Year	.vulnerabilities[].cve.published	2018	Extracted from `.vulnerabilities[].cve.id`
.vulnerabilities[].cve.references[].url	Indicator.Attribute / Vulnerability.Attribute	Reference URL	.vulnerabilities[].cve.published	https://packetstormsecurity.com/files/146131/Task-Rabbit-Clone-1.0-SQL-Injection.html	If `Reference Information` option is selected
.vulnerabilities[].cve.references[].tags[]	Indicator.Attribute / Vulnerability.Attribute	CVE Reference Tag	.vulnerabilities[].cve.published	["Exploit", "Third Party Advisory", "VDB Entry"]	N/A
.vulnerabilities[].cve.references[].source	Indicator.Attribute / Vulnerability.Attribute	CVE Reference Source	.vulnerabilities[].cve.published	MISC	N/A
.vulnerabilities[].cve.configurations[].nodes[].cpeMatch[].criteria	Indicator.Attribute / Vulnerability.Attribute	CPE	.vulnerabilities[].cve.published	cpe:2.3:a:taskrabbit_clone_project:taskrabbit_clone:1.0:*:*:*:*:*:*:*	N/A
.vulnerabilities[].cve.configurations[].nodes[].cpeMatch[].criteria	Indicator.Attribute / Vulnerability.Attribute	Affected Vendor	.vulnerabilities[].cve.published	taskrabbit_clone_project	Parsed in order to extract the needed information
.vulnerabilities[].cve.configurations[].nodes[].cpeMatch[].criteria	Indicator.Attribute / Vulnerability.Attribute	Affected Product	.vulnerabilities[].cve.published	taskrabbit_clone v1.0	Parsed in order to extract the needed information
.vulnerabilities[].cve.weaknesses[].description[].value	Indicator.Attribute / Vulnerability.Attribute	CWE	.vulnerabilities[].cve.published	CWE-89	If `CWE` option is selected
.vulnerabilities[].cve.metrics.cvssMetricV31[].impactScore	Indicator.Attribute / Vulnerability.Attribute	CVSSv31 Impact Score	.vulnerabilities[].cve.published	5.9	If `CVSS v3 Score` option is selected. If the attribute already exists, the value will be updated.
.vulnerabilities[].cve.metrics.cvssMetricV31[].exploitabilityScore	Indicator.Attribute / Vulnerability.Attribute	CVSSv31 Exploitability Score	.vulnerabilities[].cve.published	2.8	If `CVSS v3 Score` option is selected. If

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
					the attribute already exists, the value will be updated.
.vulnerabilities[].cve.metrics.cvssMetricV31[].cvssData.attackVector	Indicator.Attribute / Vulnerability.Attribute	CVSSv31 Attack Vector	.vulnerabilities[].cve.published	ADJACENT_NETWORK	If the attribute already exists, the value will be updated.
.vulnerabilities[].cve.metrics.cvssMetricV31[].cvssData.attackComplexity	Indicator.Attribute / Vulnerability.Attribute	CVSSv31 Attack Complexity	.vulnerabilities[].cve.published	LOW	If the attribute already exists, the value will be updated.
.vulnerabilities[].cve.metrics.cvssMetricV31[].cvssData.availabilityImpact	Indicator.Attribute / Vulnerability.Attribute	CVSSv31 Availability Impact	.vulnerabilities[].cve.published	HIGH	If the attribute already exists, the value will be updated.
.vulnerabilities[].cve.metrics.cvssMetricV31[].cvssData.baseScore	Indicator.Attribute / Vulnerability.Attribute	CVSSv31 Base Score	.vulnerabilities[].cve.published	6.5	If `CVSS v3 Score` option is selected. If the attribute already exists, the value will be updated.
.vulnerabilities[].cve.metrics.cvssMetricV31[].cvssData.baseSeverity	Indicator.Attribute / Vulnerability.Attribute	CVSSv31 Base Severity	.vulnerabilities[].cve.published	MEDIUM	If `Severity` option is selected. If the attribute already exists, the value will be updated.
.vulnerabilities[].cve.metrics.cvssMetricV31[].cvssData.confidentialityImpact	Indicator.Attribute / Vulnerability.Attribute	CVSSv31 Confidentiality Impact	.vulnerabilities[].cve.published	PARTIAL	If the attribute already exists, the value will be updated.
.vulnerabilities[].cve.metrics.cvssMetricV31[].cvssData.integrityImpact	Indicator.Attribute / Vulnerability.Attribute	CVSSv31 Integrity Impact	.vulnerabilities[].cve.published	HIGH	If the attribute already exists, the value will be updated.
.vulnerabilities[].cve.metrics.cvssMetricV31[].cvssData.privilegesRequired	Indicator.Attribute / Vulnerability.Attribute	CVSSv31 Privileges Required	.vulnerabilities[].cve.published	NONE	If the attribute already exists, the value will be updated.
.vulnerabilities[].cve.metrics.cvssMetricV31[].cvssData.scope	Indicator.Attribute / Vulnerability.Attribute	CVSSv31 Scope	.vulnerabilities[].cve.published	UNCHANGED	If the attribute already exists, the value will be updated.
.vulnerabilities[].cve.metrics.cvssMetricV31[].cvssData.userInteraction	Indicator.Attribute / Vulnerability.Attribute	CVSSv31 User Interaction	.vulnerabilities[].cve.published	REQUIRED	If the attribute already exists,

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
					the value will be updated.
.vulnerabilities[].cve.metrics.cvssMetricV31[].cvssData.vectorString	Indicator.Attribute / Vulnerability.Attribute	CVSSv31 Vector String	.vulnerabilities[].cve.published	CVSS:3.0/AV:A/AC:L/PR:N/C:N/I:H/A:H	If the attribute already exists, the value will be updated.
.vulnerabilities[].cve.metrics.cvssMetricV31[].cvssData.version	Indicator.Attribute / Vulnerability.Attribute	CVSSv31 Version	.vulnerabilities[].cve.published	3.1	If the attribute already exists, the value will be updated.
.vulnerabilities[].cve.metrics.cvssMetricV30[].impactScore	Indicator.Attribute / Vulnerability.Attribute	CVSSv30 Impact Score	.vulnerabilities[].cve.published	5.9	If `CVSS v3 Score` option is selected. If the attribute already exists, the value will be updated.
.vulnerabilities[].cve.metrics.cvssMetricV30[].exploitabilityScore	Indicator.Attribute / Vulnerability.Attribute	CVSSv30 Exploitability Score	.vulnerabilities[].cve.published	2.8	If `CVSS v3 Score` option is selected. If the attribute already exists, the value will be updated.
.vulnerabilities[].cve.metrics.cvssMetricV30[].cvssData.attackVector	Indicator.Attribute / Vulnerability.Attribute	CVSSv30 Attack Vector	.vulnerabilities[].cve.published	ADJACENT_NETWORK	If the attribute already exists, the value will be updated.
.vulnerabilities[].cve.metrics.cvssMetricV30[].cvssData.attackComplexity	Indicator.Attribute / Vulnerability.Attribute	CVSSv30 Attack Complexity	.vulnerabilities[].cve.published	LOW	If the attribute already exists, the value will be updated.
.vulnerabilities[].cve.metrics.cvssMetricV30[].cvssData.availabilityImpact	Indicator.Attribute / Vulnerability.Attribute	CVSSv30 Availability Impact	.vulnerabilities[].cve.published	HIGH	If the attribute already exists, the value will be updated.
.vulnerabilities[].cve.metrics.cvssMetricV30[].cvssData.baseScore	Indicator.Attribute / Vulnerability.Attribute	CVSSv30 Base Score	.vulnerabilities[].cve.published	6.5	If `CVSS v3 Score` option is selected. If the attribute already exists, the value will be updated.
.vulnerabilities[].cve.metrics.cvssMetricV30[].cvssData.baseSeverity	Indicator.Attribute / Vulnerability.Attribute	CVSSv30 Base Severity	.vulnerabilities[].cve.published	MEDIUM	If `Severity` option is selected. If the attribute already exists, the value will be updated.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.vulnerabilities[].cve.metrics.cvssMetricV30[].cvssData.confidentialityImpact	Indicator.Attribute / Vulnerability.Attribute	CVSSv30 Confidentiality Impact	.vulnerabilities[].cve.published	PARTIAL	If the attribute already exists, the value will be updated.
.vulnerabilities[].cve.metrics.cvssMetricV30[].cvssData.integrityImpact	Indicator.Attribute / Vulnerability.Attribute	CVSSv30 Integrity Impact	.vulnerabilities[].cve.published	HIGH	If the attribute already exists, the value will be updated.
.vulnerabilities[].cve.metrics.cvssMetricV30[].cvssData.privilegesRequired	Indicator.Attribute / Vulnerability.Attribute	CVSSv30 Privileges Required	.vulnerabilities[].cve.published	NONE	If the attribute already exists, the value will be updated.
.vulnerabilities[].cve.metrics.cvssMetricV30[].cvssData.scope	Indicator.Attribute / Vulnerability.Attribute	CVSSv30 Scope	.vulnerabilities[].cve.published	UNCHANGED	If the attribute already exists, the value will be updated.
.vulnerabilities[].cve.metrics.cvssMetricV30[].cvssData.userInteraction	Indicator.Attribute / Vulnerability.Attribute	CVSSv30 User Interaction	.vulnerabilities[].cve.published	REQUIRED	If the attribute already exists, the value will be updated.
.vulnerabilities[].cve.metrics.cvssMetricV30[].cvssData.vectorString	Indicator.Attribute / Vulnerability.Attribute	CVSSv30 Vector String	.vulnerabilities[].cve.published	CVSS:3.0/AV:A/AC:L/PR:N/C:N/I:H/A:H	If the attribute already exists, the value will be updated.
.vulnerabilities[].cve.metrics.cvssMetricV30[].cvssData.version	Indicator.Attribute / Vulnerability.Attribute	CVSSv30 Version	.vulnerabilities[].cve.published	3.0	If the attribute already exists, the value will be updated.

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.

METRIC	RESULT
Run Time	1 minute
Indicators	142
Indicator Attributes	1,999
Vulnerabilities	142
Vulnerability Attributes	1,999

Known Issues / Limitations

- The maximum allowable range is 120 consecutive days. If a larger date range is selected, the feed will change the end date to start date plus 120 days.
- A delay between calls exists to avoid NIST firewall rules rejecting the requests due to the imposed rate limit. Requesting an API key significantly raises the number of requests that can be made in a given time frame and the feed will run faster. You can enter the API Key on the integration's configuration page.

Change Log

- **Version 3.0.3**
  - The integration no longer ingests CVSSv2 attributes.
  - The CDF now updates CVSS attributes instead of creating new ones in the event that the attribute has been updated.
- **Version 3.0.2**
  - Added the ability to call the API using an API Key. This will allow for more requests in a given time frame. See the Known Issues / Limitations chapter for more details.
  - Added two new configuration options:
    - API Key
    - For Each Vulnerability Found Return the Following
- **Version 3.0.1**
  - Resolved a bug that appears on the first run.
- **Version 3.0.0**
  - Updated the feed to use the NVD 2.0.0 API
  - Added new configuration options:
    - Date used for Filtering the Data
    - CVSSv3 Severity Rating
    - Filter the results based on Keyword
    - Use Keyword Exact Match
- **Version 2.2.3**
  - Fixed an attribute scoring bug where scoring attributes with a value of 0 were not created.
- **Version 2.2.2**
  - Added description to indicators and vulnerabilities.
- **Version 2.2.1**
  - Documentation updates and more attributes added
- **Version 2.2.0**
  - Update endpoint for NVD's change, `/cve/1.0/nvdcve-1.0-` --> `/cve/1.1/nvdcve-1.1-`
- **Version 2.1.0**

    - Added missing objects attributes
- **Version 2.0.0**
    - Initial release