ThreatQuotient

National Vulnerability Database (NVD) CVE Feed Guide

Version 2.2.1

July 13, 2021

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

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

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.

Contents

Versioning

- Current integration version: `2.2.1`
- Supported on ThreatQ versions >= `4.27.0`

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.

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 **NVD** feed 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
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.

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.

NVD data is returned in the following format:

`GET https://nvd.nist.gov/feeds/json/cve/1.1/nvdcve-1.1-<YEAR>.json.gz`


```
{
  "CVE_data_type" : "CVE",
  "CVE_data_format" : "MITRE",
  "CVE_data_version" : "4.0",
  "CVE_data_numberOfCVEs" : "1",
  "CVE_data_timestamp" : "2021-06-08T07:02Z",
  "CVE_Items" : [
    {
      "publishedDate" : "2018-01-29T05:29Z",
      "lastModifiedDate" : "2020-03-11T18:41Z",
      "impact" : {
        "baseMetricV2" : {
          "obtainAllPrivilege" : false,
          "userInteractionRequired" : false,
          "impactScore" : 6.4,
          "cvssV2" : {
            "authentication" : "NONE",
            "integrityImpact" : "PARTIAL",
            "vectorString" : "AV:N/AC:L/Au:N/C:P/I:P/A:P",
            "accessComplexity" : "LOW",
            "confidentialityImpact" : "PARTIAL",
            "baseScore" : 7.5,
            "version" : "2.0",
            "availabilityImpact" : "PARTIAL",
            "accessVector" : "NETWORK"
          },
          "acInsufInfo" : true,
          "exploitabilityScore" : 10.0,
          "severity" : "HIGH",
          "obtainOtherPrivilege" : false,
          "obtainUserPrivilege" : false
        },
        "baseMetricV3": {
```

```
      "cvssV3": {
        "attackVector": "ADJACENT_NETWORK",
        "vectorString": "CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H",
        "baseSeverity": "HIGH",
        "integrityImpact": "HIGH",
        "scope": "UNCHANGED",
        "baseScore": 8.8,
        "confidentialityImpact": "HIGH",
        "attackComplexity": "LOW",
        "version": "3.0",
        "availabilityImpact": "HIGH",
        "userInteraction": "NONE",
        "privilegesRequired": "NONE"
      },
      "impactScore": 5.9,
      "exploitabilityScore": 2.8
    },
  },
  "cve" : {
    "affects" : {
      "vendor" : {
        "vendor_data" : [
          {
            "product" : {
              "product_data" : [
                {
                  "version" : {
                    "version_data" : [
                      {
                        "version_value" : "1.0",
                        "version_affected" : "="
                      }
                    ]
                  },
                  "product_name" : "taskrabbit_clone"
                }
              ]
            },
            "vendor_name" : "taskrabbit_clone_project"
          }
        ]
      }
    },
    "references" : {
      "reference_data" : [
        {
          "url" : "https://packetstormsecurity.com/files/146131/Task-Rabbit-Clone-1.0-SQL-Injection.html",
          "name" : "https://packetstormsecurity.com/files/146131/Task-Rabbit-Clone-1.0-SQL-Injection.html",
          "tags" : [
            "Exploit",
            "Third Party Advisory",
            "VDB Entry"
          ],
          "refsource" : "MISC"
        },
        {
          "url" : "https://www.exploit-db.com/exploits/43914/",
          "name" : "43914",
          "tags" : [
            "Exploit",
```

```
              "Third Party Advisory",
              "VDB Entry"
            ],
            "refsource" : "EXPLOIT-DB"
          }
        ]
      },
      "data_type" : "CVE",
      "description" : {
        "description_data" :
        [
          {
            "lang" : "en",
            "value" : "SQL Injection exists in Task Rabbit Clone 1.0 via the single_blog.php id parameter."
          }
        ]
      },
      "CVE_data_meta" : {
        "ASSIGNER" : "cve@mitre.org",
        "ID" : "CVE-2018-6363"
      },
      "data_format" : "MITRE",
      "problemtype" : {
        "problemtype_data" : [
          {
            "description" : [
              {
                "lang" : "en",
                "value" : "CWE-89"
              }
            ]
          }
        ]
      },
      "data_version" : "4.0"
    },
    "configurations" : {
      "nodes" : [
        {
          "cpe_match" : [
            {
              "cpe23Uri" : "cpe:2.3:a:taskrabbit_clone_project:taskrabbit_clone:1.0:*:*:*:*:*:*:*",
              "vulnerable" : true
            }
          ],
          "operator" : "OR"
        }
      ],
      "CVE_data_version" : "4.0"
    }
  }
]
}
```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.CVE_Items[].cve.CVE_data_meta.ID	Indicator.Value / Vulnerability.Value	CVE / N/A	.CVE_Items[].publishedDate	CVE-2018-6363	
.CVE_Items[].cve.description.description_data[].value	Vulnerability.Attribute / Indicator.Attribute	Description	.CVE_items[].publishedDate	SQL Injection exists in Task RabbitClone 1.0 via the single_blog.php id parameter.	
.CVE_Items[].cve.CVE_data_meta.ID	Vulnerability.Attribute / Indicator.Attribute	Year	N/A	2018	Extracts the year section
.CVE_Items[].cve.references.reference_data[].url	Vulnerability.Attribute / Indicator.Attribute	Reference URL	.CVE_items[].publishedDate	https://packetstormsecurity.com/files/146131/Task-Rabbit-Clone-1.0-SQL-Injection.html	
.CVE_Items[].impact.baseMetricV2.severity	Vulnerability.Attribute / Indicator.Attribute	CVSSv2 Severity	.CVE_items[].publishedDate	HIGH	
.CVE_Items[].impact.baseMetricV2.exploitabilityScore	vulnerability.attribute / Indicator.Attribute	CVSSv2 Exploitability Score	.CVE_items[].publishedDate	10.0	
.CVE_Items[].impact.baseMetricV2.impactScore	Vulnerability.Attribute / Indicator.Attribute	CVSSv2 Impact Score	.CVE_items[].publishedDate	6.4	
.CVE_Items[].impact.baseMetricV3.impactScore	Vulnerability.Attribute / Indicator.Attribute	CVSSv3 Impact Score	.CVE_items[].publishedDate	5.9	
.CVE_Items[].impact.baseMetricV3.exploitabilityScore	Vulnerability.Attribute / Indicator.Attribute	CVSSv3 Exploitability Score	.CVE_items[].publishedDate	2.8	
.CVE_Items[].configuration.nodes[].cpe_match[].cpe23Uri	Vulnerability.Attribute / Indicator.Attribute	CPE	.CVE_items[].publishedDate	cpe:2.3:a:taskrabbit_clone_project:taskrabbit_clone:1.0:*:*:*:*:*:*:*	
.CVE_Items[].cve.affects.vendor.vendor_data[].product.product_data[].product_name	Vulnerability.Attribute / Indicator.attribute	Product	.CVE_items[].publishedDate	ace_server	
.CVE_Items[].cve.affects.vendor.vendor_data[].vendor_name	Vulnerability.Attribute / Indicator.Attribute	Vendor Name	.CVE_items[].publishedDate	rsa	
.CVE_Items[].cve.references.reference_data[].tags[]	Vulnerability.Attribute / Indicator.Attribute	CVE Reference Tag	.CVE_items[].publishedDate	["Exploit", "Third Party Advisory","VDB Entry"]	
.CVE_Items[].cve.references.reference_data[].refsource	Vulnerability.Attribute / Indicator.Attribute	CVE Reference Source	.CVE_items[].publishedDate	MISC	
.CVE_Items[].cve.references.reference_data[].name	Vulnerability.Attribute / Indicator.Attribute	CVE Reference Name	.CVE_items[].publishedDate	https://packetstormsecurity.com/files/146131/Task-Rabbit-Clone-1.0-SQL-Injection.html	

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.CVE_Items[].cve.problemtype.problemtype_data[].description[].value	Vulnerability.Attribute / Indicator.Attribute	CVE Problem Type	.CVE_items[].publishedDate	CWE-89	
.CVE_Items[].configuration.CVE_data_version	Vulnerability.Attribute / Indicator.Attribute	CVE Data Version	.CVE_items[].publishedDate	4.0	
.CVE_Items[].cve.data_format	Vulnerability.Attribute / Indicator.Attribute	CVE Data Format	.CVE_items[].publishedDate	Mitre	
.CVE_Items[].cve.data_type	Vulnerability.Attribute / Indicator.Attribute	CVE Data Type	.CVE_items[].publishedDate	CVE	
.CVE_Items[].cve.CVE_data_meta.ASSIGNER	Vulnerability.Attribute / Indicator.Attribute	CVE Data Meta Assigner	.CVE_items[].publishedDate	cve@mitre.org	
.CVE_Items[].cve.configuration.nodes[].cpe23_match[].cpe23Uri	Vulnerability.Attribute / Indicator.Attribute	Affected Vendor	.CVE_items[].publishedDate	taskrabbit_clone_project	Is determined based on the splitting of `.cve.configuration.nodes[].cpe23_match[].cpe23Uri` after `:`and taking the 4'th element
.CVE_Items[].cve.configuration.nodes[].cpe23_match[].cpe23Uri	Vulnerability.Attribute / Indicator.Attribute	Affected Product	.CVE_items[].publishedDate	taskrabbit_clone	Is determined based on the splitting of `.cve.configuration.nodes[].cpe23_match[].cpe23Uri` after `:` and taking the 5'th and 6'th element
.CVE_Items[].impact.baseMetricV2.cvssV2.accessComplexity	Vulnerability.Attribute / Indicator.Attribute	CVSSv2 Access Complexity	.CVE_items[].publishedDate	MEDIUM	
.CVE_Items[].impact.baseMetricV2.cvssV2.accessVector	Vulnerability.Attribute / Indicator.Attribute	CVSSv2 Access Vector	.CVE_items[].publishedDate	NETWORK	
.CVE_Items[].impact.baseMetricV2.cvssV2.authentication	Vulnerability.Attribute / Indicator.Attribute	CVSSv2 Authentication	.CVE_items[].publishedDate	SINGLE	
.CVE_Items[].impact.baseMetricV2.cvssV2.availabilityImpact	Vulnerability.Attribute / Indicator.Attribute	CVSSv2 Availability Impact	.CVE_items[].publishedDate	PARTIAL	

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.CVE_Items[].impact.base MetricV2.cvssV2.baseScore	Vulnerability.attribute / Indicator.Attribute	CVSSv2 Base Score	.CVE_items[].publishedDate	4.3	
.CVE_Items[].impact.base MetricV2.cvssV2.confidentiality Impact	Vulnerability.Attribute / Indicator.Attribute	CVSSv2 Confidentiality Impact	.CVE_items[].publishedDate	COMPLETE	
.CVE_Items[].impact.base MetricV2.cvssV2.integrity Impact	Vulnerability.Attribute / Indicator.Attribute	CVSSv2 Integrity Impact	.CVE_items[].publishedDate	COMPLETE	
.CVE_Items[].impact.base MetricV2.cvssV2.vectorString	Vulnerability.attribute / Indicator.Attribute	CVSSv2 Vector String	.CVE_items[].publishedDate	AV:N/AC:M/Au:N/C:N/I: N/A:P	
.CVE_Items[].impact.base MetricV2.cvssV2.version	Vulnerability.Attribute / Indicator.Attribute	CVSSv2 Version	.CVE_items[].publishedDate	2.0	
.CVE_Items[].impact.base MetricV2.userInteraction Required	Vulnerability.Attribute / Indicator.Attribute	CVSSv2 User Interaction Required	.CVE_items[].publishedDate	false	
.CVE_Items[].impact.base MetricV2.obtainOtherPrivilege	Vulnerability.Attribute / Indicator.Attribute	CVSSv2 Obtain Other Privilege	.CVE_items[].publishedDate	false	
.CVE_Items[].impact.baseMetricV2. obtainUserPrivilege	Vulnerability.Attribute / Indicator.Attribute	CVSSv2 Obtain User Privilege	.CVE_items[].publishedDate	false	
.CVE_Items[].impact.baseMetricV2. obtainAllPrivilege	Vulnerability.Attribute / Indicator.Attribute	CVSSv2 Obtain All Privilege	.CVE_items[].publishedDate	false	
.CVE_Items[].impact.baseMetricV2. acInsufInfo	Vulnerability.Attribute / Indicator.Attribute	CVSSv2 AC Insuf Info	.CVE_items[].publishedDate	true	
.CVE_Items[].impact.baseMetricV3. cvssV3.attackVector	Vulnerability.Attribute / Indicator.Attribute	CVSSv3 Attack Vector	.CVE_items[].publishedDate	ADJACENT_NETWORK	
.CVE_Items[].impact.baseMetricV3. cvssV3.attackComplexity	Vulnerability.Attribute / Indicator.Attribute	CVSSv3 Attack Complexity	.CVE_items[].publishedDate	LOW	
.CVE_Items[].impact.baseMetricV3. cvssV3.availabilityImpact	Vulnerability.Attribute / Indicator.Attribute	CVSSv3 Availability Impact	.CVE_items[].publishedDate	HIGH	
.CVE_Items[].impact.baseMetricV3. cvssV3.baseScore	Vulnerability.Attribute / Indicator.Attribute	CVSSv3 Base Score	.CVE_items[].publishedDate	6.5	
.CVE_Items[].impact.baseMetricV3. cvssV3.baseSeverity	Vulnerability.Attribute / Indicator.Attribute	CVSSv3 Base Severity	.CVE_items[].publishedDate	MEDIUM	
.CVE_Items[].impact.baseMetricV3. cvssV3.confidentialityImpact	Vulnerability.Attribute / Indicator.Attribute	CVSSv3 Confidentiality Impact	.CVE_items[].publishedDate	PARTIAL	
.CVE_Items[].impact.baseMetricV3. cvssV3.integrityImpact	Vulnerability.Attribute / Indicator.Attribute	CVSSv3 Integrity Impact	.CVE_items[].publishedDate	HIGH	
.CVE_Items[].impact.baseMetricV3. cvssV3.privilegesRequired	Vulnerability.Attribute / Indicator.Attribute	CVSSv3 Privileges Required	.CVE_items[].publishedDate	NONE	
.CVE_Items[].impact.baseMetricV3. cvssV3.scope	Vulnerability.Attribute / Indicator.Attribute	CVSSv3 Scope	.CVE_items[].publishedDate	UNCHANGED	
.CVE_Items[].impact.baseMetricV3. cvssV3.userInteraction	Vulnerability.attribute / Indicator.Attribute	CVSSv3 User Interaction	.CVE_items[].publishedDate	REQUIRED	

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.CVE_Items[].impact.baseMetricV3.cvssV3.vectorString	Vulnerability.attribute / Indicator.Attribute	CVSSv3 Vector String	.CVE_items[].publishedDate	AV:N/AC:M/Au:N/C:N/I:N/A:P	
.CVE_Items[].impact.baseMetricV3.cvssV3.version	Vulnerability.Attribute / Indicator.Attribute	CVSSv3 Version	.CVE_items[].publishedDate	2.0	

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. Manual feed runs may take significantly longer than scheduled runs to complete due to ingesting one or multiple years' worth of data in a single feed run.

Scheduled run ingesting CVE data as CVE Indicators (default configuration)

METRIC	RESULT
Run Time	5 minutes
Indicators	1,171
Indicator Attributes	16,817

Scheduled run ingesting CVE data as CVE Indicators and Vulnerabilities

METRIC	RESULT
Run Time	7 minutes
Indicators	1,171
Indicator Attributes	16,817
Vulnerabilities	1,171
Vulnerability Attributes	16,817

Known Issues/Limitations

CVE-2002 is the oldest vulnerability feed provided by NVD. However, vulnerability data from years 2001, 2000, and 1999 are also included in the 2002 feed. When triggering a manual run, specifying a `Start Date` prior to 2002 will result in requesting data from the CVE-2002 feed.

Change Log

- **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