ThreatQuotient

National Vulnerability Database (NVD) CVE Feed Implementation Guide

Version 2.2.0

Monday, September 21, 2020

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.

Last Updated: Monday, September 21, 2020

Contents

Versioning

- Current integration version: `2.2.0`
- 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 feed:

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

1. Log into https://marketplace.threatq.com/.
2. Locate and download the **NVD** feed file.
3. Navigate to your ThreatQ instance.
4. Click on the **Settings** icon and select **Incoming feeds**.
5. Click on the **Add New Feed** button.
6. Upload the feed file using one of the following methods:
   - Drag and drop the file into the dialog box
   - Select **Click to Browse** to locate the feed 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.

The feed will be added to the **OSINT** tab for Incoming Feeds. 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 feed-related credentials.

To configure the feed:

1. Click on the **Settings** icon and select **Incoming Feeds**.
2. Locate the feed under the **OSINT** tab.
3. Click on the **Feed Settings** link for the feed.
4. Under the **Connection** tab, enter the following configuration parameters:

Parameter	Description
Save CVE Data as	This parameter is required and can be configured to have the feed ingest CVE data as indicators, vulnerabilities, or both. This parameter is required.
Verify SSL Certificate	Whether to verify the server's SSL Certificate.

5. Click on **Save Changes**.
6. Click on the toggle switch to the left of the feed name to enable the feed.

ThreatQ Mapping

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`

```
{
  "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-Injec-
tion.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.CVE_data.meta.ID	vulnerability.value	N/A	.pub-lishedDate	CVE-2018-6363	
.cve.CVE_data.meta.ID	indicator.value	CVE	.pub-lishedDate	CVE-2018-6363	
.cve.-description.description_data[0].value	vul-ner-ability.description / vul-ner-ability.description	N/A	.pub-lishedDate	SQL Injection exists in Task Rabbit Clone 1.0 via the single_blog.php id parameter.	
N/A	vul-nerability.attribute / indicator.attribute	Year	N/A	2018	Extracted from the CVE ID found at

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
					.cve.CVE_data.-meta.ID
.cve.ref-erences.reference_data[].url	vul-nerability.attribute / indicator.attribute	Reference URL	.pub-lishedDate	https://pack-etstormsecurity.com/files/146131/Task-Rab-bit-Clone-1.0-SQL-Injection.html	
.im-pact.-baseMetricV2.severity	vul-nerability.attribute / indicator.attribute	CVSSv2 Severity	.pub-lishedDate	HIGH	
.impact.baseMetricV2.exploitabilityScore	vul-nerability.attribute / indicator.attribute	CVSSv2 Exploit-ability Score	.pub-lishedDate	10.0	
.impact.baseMetricV2.impactScore	vul-nerability.attribute / indicator.attribute	CVSSv2 Impact Score	.pub-lishedDate	6.4	

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
.impact.baseMetricV3.impactScore	vulnerability.attribute / indicator.attribute	CVSSv3 Impact Score	.publishedDate	5.9	
.impact.baseMetricV3.exploitabilityScore	vulnerability.attribute / indicator.attribute	CVSSv3 Exploitability Score	.publishedDate	2.8	
.configuration.nodes[].cpe_match[].cpe23Uri	vulnerability.attribute / indicator.attribute	CPE	.publishedDate	cpe:2.3:a:taskrabbit_clone_project:taskrabbit_clone:1.0:*:*:*:*:*:*:*	
.cve.affects.vendor.vendor_data[].product.product_data[].product_name	vulnerability.attribute / indicator.attribute	Product	.publishedDate	ace_server	
.cve.affects.vendor.vendor_data[].vendor_name	vulnerability.attribute / indicator.attribute	Vendor Name	.publishedDate	rsa	

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
.impact.baseMetricV2.cvssV2.accessComplexity	vulnerability.attribute / indicator.attribute	CVSSv2 Access Complexity	.publishedDate	MEDIUM	
.impact.baseMetricV2.cvssV2.accessVector	vulnerability.attribute / indicator.attribute	CVSSv2 Access Vector	.publishedDate	NETWORK	
.impact.baseMetricV2.cvssV2.authentication	vulnerability.attribute / indicator.attribute	CVSSv2 Authentication	.publishedDate	SINGLE	
.impact.baseMetricV2.cvssV2.availabilityImpact	vulnerability.attribute / indicator.attribute	CVSSv2 Availability Impact	.publishedDate	PARTIAL	
.impact.baseMetricV2.cvssV2.baseScore	vulnerability.attribute / indicator.attribute	CVSSv2 Base Score	.publishedDate	4.3	

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
.impact.baseMetricV2.cvssV2.-confidentialityImpact	vul-nerability.attribute / indicator.attribute	CVSSv2 Con-fidentiality Impact	.pub-lishedDate	COMPLETE	
.impact.baseMetricV2.cvssV2.integrityImpact	vul-nerability.attribute / indicator.attribute	CVSSv2 Integrity Impact	.pub-lishedDate	COMPLETE	
.impact.baseMetricV2.cvssV2.vectorString	vul-nerability.attribute / indicator.attribute	CVSSv2 Vector String	.pub-lishedDate	AV:N/AC:M/Au:N/C:N/I:N/A:P	
.impact.baseMetricV2.cvssV2.version	vul-nerability.attribute / indicator.attribute	CVSSv2 Version	.pub-lishedDate	2.0	
.impact.baseMetricV3.cvssV3.attackVector	vul-nerability.attribute / indicator.attribute	CVSSv3 Attack Vector	.pub-lishedDate	ADJACENT_NETWORK	

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
.impact.baseMetricV3.cvssV3.attackComplexity	vulnerability.attribute / indicator.attribute	CVSSv3 Attack Complexity	.publishedDate	LOW	
.impact.baseMetricV3.cvssV3.availabilityImpact	vulnerability.attribute / indicator.attribute	CVSSv3 Availability Impact	.publishedDate	HIGH	
.impact.baseMetricV3.cvssV3.baseScore	vulnerability.attribute / indicator.attribute	CVSSv3 Base Score	.publishedDate	6.5	
.impact.baseMetricV3.cvssV3.baseSeverity	vulnerability.attribute / indicator.attribute	CVSSv3 Base Severity	.publishedDate	MEDIUM	
.impact.baseMetricV3.cvssV3.-confidentialityImpact	vulnerability.attribute / indicator.attribute	CVSSv3 Confidentiality Impact	.publishedDate	PARTIAL	

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
.impact.baseMetricV3.cvssV3.integrityImpact	vulnerability.attribute / indicator.attribute	CVSSv3 Integrity Impact	.publishedDate	HIGH	
.impact.baseMetricV3.cvssV3.privilegesRequired	vulnerability.attribute / indicator.attribute	CVSSv3 Privileges Required	.publishedDate	NONE	
.impact.baseMetricV3.cvssV3.scope	vulnerability.attribute / indicator.attribute	CVSSv3 Scope	.publishedDate	UNCHANGED	
.impact.baseMetricV3.cvssV3.userInteraction	vulnerability.attribute / indicator.attribute	CVSSv3 User Interaction	.publishedDate	REQUIRED	
.impact.baseMetricV3.cvssV3.vectorString	vulnerability.attribute / indicator.attribute	CVSSv3 Vector String	.publishedDate	AV:N/AC:M/Au:N/C:N/I:N/A:P	

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
.impact.baseMetricV3.cvssV3.version	vulnerability.attribute / indicator.attribute	CVSSv3 Version	.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.

NVD CVE: Scheduled run ingesting CVE data as CVE Indicators (default configuration).

Metric	Result
Run Time	5 minutes
Indicators	1,171
Indicator Attributes	16,817

NVD CVE: 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 2.2.0**
  - Updated the endpoint to reflect NVD's change, `/cve/1.0/nvdcve-1.0-` --> `/cve/1.1/nvdcve-1.1-`
- **Version 2.1.0**
  - Added user configuration parameters to ingest CVEs as indicators, vulnerabilities, or both.
  - Added manual run support.
- **Version 2.0.1**
  - Added vulnerability attributes to indicators.
  - Added report support for `Vendor Name` and `Product` attributes.
- **Version 2.0.0**
  - Initial release as a CDF.