ThreatQuotient

National Vulnerability Database (NVD) CVE Feed Implementation Guide

Version 2.1.0

Tuesday, April 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: Tuesday, April 21, 2020

Contents

Versioning

- Current integration version: `2.1.0`
- 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.

Feed Runs

The following section describes how information is ingested into the ThreatQ platform via scheduled and manual feed runs.

Scheduled Runs

The feed will automatically initiate a scheduled run when it is first enabled. The feed will pull from NVD's CVE Modified feed which contains CVE data that has been recently published or modified within the last 8 days.

Ingest for a Specific Year (Manual Runs)

You can ingest CVEs for a specific year by performing a manual run via the **Run Feed** option.

From the **Feed Settings** section for the NVD CVE feed:

1. Click on the **Run Feed** button.

   The Trigger Manual Run dialog box opens.

2. Select the desired **year** from the dropdown provided.

> ⚠ The Month, Day, and Time fields are not used with this feed. This is due to how NVD organizes its data, which is by year. By selecting a year, the connector will pull down a package with all data for that specific year.
>
> 2002 is the earliest year that NVD has a feed created for users to pull and contains data from 2002 and all years prior. Selecting **2002** will not only pull data from that year but also all data published prior to 2002. Selecting a year prior to 2002 will result in pulling the

⚠ NVD 2002 feed which includes the previous years' data as well.

3. Click on **Queue Run**.

ThreatQ Mapping

NVD CVE

Scheduled runs ingest CVE data from the "modified" package. Manual runs will request the package for each year in the range specified by the `Start Date` and `End Date` parameters. When triggering a manual run, only the year field of the `Start Date` and `End Date` parameters is evaluated.

Ingested CVE data can be mapped as indicators (default configuration), vulnerabilities, or both.

NVD data is returned in the following format:

```
{
  "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://pack-
etstormsecurity.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
```

```
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:taskrabb
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
.cve.CVE_data.meta.ID	Vulnerability.value	N/A	.publishedDate	CVE-2018-6363
.cve.CVE_data.meta.ID	Indicator.value	CVE	.publishedDate	CVE-2018-6363
.cve.description.description_data[0].value	Vulnerability.description	N/A	.publishedDate	SQL Injection exists in Task Rabbit Clone 1.0 via the single_blog.php id parameter.
.cve.description.description_data[0].value	Indicator.Attribute	Description	.publishedDate	SQL Injection exists in Task Rabbit Clone 1.0 via the single_blog.php id parameter.
N/A	Vulnerability.Attribute / Indicator.Attribute	Year	N/A	2018
.cve.references.reference_data[].url	Vulnerability.Attribute / Indicator.Attribute	Reference URL	.publishedDate	https://packetstormsecurity.com/files/146131/Task-Rab-

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples
				bit-Clone-1.0-SQL-Injection.html
.impact.baseMetricV2.severity	Vulnerability.Attribute / Indicator.Attribute	CVSSv2 Severity	.publishedDate	HIGH
.impact.baseMetricV2.exploitabilityScore	Vulnerability.Attribute / Indicator.Attribute	CVSSv2 Exploitability Score	.publishedDate	10.0
.impact.baseMetricV2.impactScore	Vulnerability.Attribute / Indicator.Attribute	CVSSv2 Impact Score	.publishedDate	6.4
.impact.baseMetricV3.impactScore	Vulnerability.Attribute / Indicator.Attribute	CVSSv3 Impact Score	.publishedDate	5.9
.im-	Vulnerability.Attribute	CVSSv3	.pub-	2.8

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples
pact.baseMetricV3.exploitabilityScore	/ Indicator.Attribute	Exploitability Score	lishedDate	
.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

Average Feed Run

CVE Save As	Run Time (minutes)	Indicators	Indicator Attributes	Vulnerabilities	Vulnerability Attributes
Indicators (default)	5	1,171	16,817	N/A	N/A
Indicators and Vulnerabilities	7	1,171	16,817	1,171	16,817
Object counts and Feed run time are supplied as generalities only - objects returned by a provider can differ based on credential configurations and Feed run time may vary based on system resources and load.					

Change Log

- **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.