

# ThreatQuotient



## National Vulnerability Database (NVD) Feed Implementation Guide

**Version 2.0.0**

Tuesday, March 24, 2020

**ThreatQuotient**

11400 Commerce Park Dr., Suite 200

Reston, VA 20191

### **Support**

Email: [support@threatq.com](mailto:support@threatq.com)

Web: [support.threatq.com](http://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.

Copyright © 2020 ThreatQuotient, Inc.

All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

Last Updated: Tuesday, March 24, 2020

# Contents

National Vulnerability Database (NVD) Feed Implementation Guide .....	1
Warning and Disclaimer .....	2
Contents .....	3
Versioning .....	4
Introduction .....	5
Installation .....	6
Configuration .....	7
ThreatQ Mapping .....	8
NVD CVE .....	8
Average Feed Run .....	17

# Versioning

- Current integration version: 2.0.0
- Supported on ThreatQ versions  $\geq$  4.27.0

# Introduction

The National Vulnerability Database (NVD) 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 are provided in the "modified" package. Currently, historic records are available for all years between 2010-2019.

# 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
Target Year	<p>This dropdown parameter is required. This field can be configured to have the feed ingest either all newly published CVEs and CVE updates via the <b>Latest</b> option, or all CVEs for a given historic year. The feed will only need to be run once when pulling data for a historic year.</p> <div> If running the Feed on a Scheduled basis, the <b>Latest</b> option should be used.</div>
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

## NVD CVE

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://pack-
etstormsecurity.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 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
.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	Reference URL	.publishedDate	<a href="https://packetstormsecurity.com/files/146131/Task-Rab-">https://packetstormsecurity.com/files/146131/Task-Rab-</a>

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	CVSSv2 Exploitability Score	.publishedDate	10.0
.impact.baseMetricV2.impactScore	Vulnerability.Attribute	CVSSv2 Impact Score	.publishedDate	6.4
.impact.baseMetricV3.impactScore	Vulnerability.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		Exploitability Score	lishedDate	
.configuration.nodes[].cpe_match[].cpe23Uri	Vulnerability.Attribute	CPE	.publishedDate	cpe:2.3:a:taskrabbit_clone_project:taskrabbit_clone:1.0:xxxxx*



## Average Feed Run

Target Year	Run Time (minutes)	Indicators	Indicator Attributes	Vulnerabilities	Vulnerability Attributes
Latest	2	960	2,718	960	9,062
2019	47	14,929	43,874	14,929	153,535
2018	45	16,077	47,379	16,077	185,228
2017	54	15,968	45,987	15,968	216,808
2016	33	10,265	29,659	10,265	195,104
2015	30	8,488	24,864	8,488	158,127
2014	39	8824	25,915	8,824	201,050
2013	44	6,617	19,355	6,617	231,132
2012	49	5,789	16,985	5,789	230,804
2011	132	4,806	14,200	4,806	732,404
2010	48	5,168	15,362	5,168	250,455
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.					