# ThreatQuotient

## National Vulnerability Database (NVD) CVE Action Guide

**Version 1.0.2**

May 30, 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** | 1.0.2 |
| **Compatible with ThreatQ Versions** | >= 5.12.1 |
| **ThreatQ TQO License Required** | Yes |
| **Support Tier** | ThreatQ Supported |

# Introduction

The National Vulnerability Database (NVD) CVE action submits a ThreatQ data collection, consisting of CVEs and Vulnerabilities, to NVD for enrichment.  NVD returns detailed information that is then ingested back into ThreatQ.

The integration provides the following action:

- **NVD CVE** - submits CVEs and Vulnerabilities to be enriched.

The action is compatible with the following system objects:

- CVEs (indicators)
- Vulnerabilities

The action returns the following enriched system objects:

- Indicators
  - Indicator attributes
- Vulnerabilities
  - Vulnerability Attributes

This action is intended for use with ThreatQ TDR Orchestrator (TQO). An active TQO license is required for this feature.

# Prerequisites

- An active ThreatQ TDR Orchestrator (TQO) license.
- A data collection containing at least of the of the following object types:
  - CVE (indicator)
  - Vulnerability

# 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 action zip file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the action 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 action already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the action contains changes to the user configuration. The new user configurations will overwrite the existing ones for the action and will require user confirmation before proceeding.

You will still need to configure the action.

# Configuration

> ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

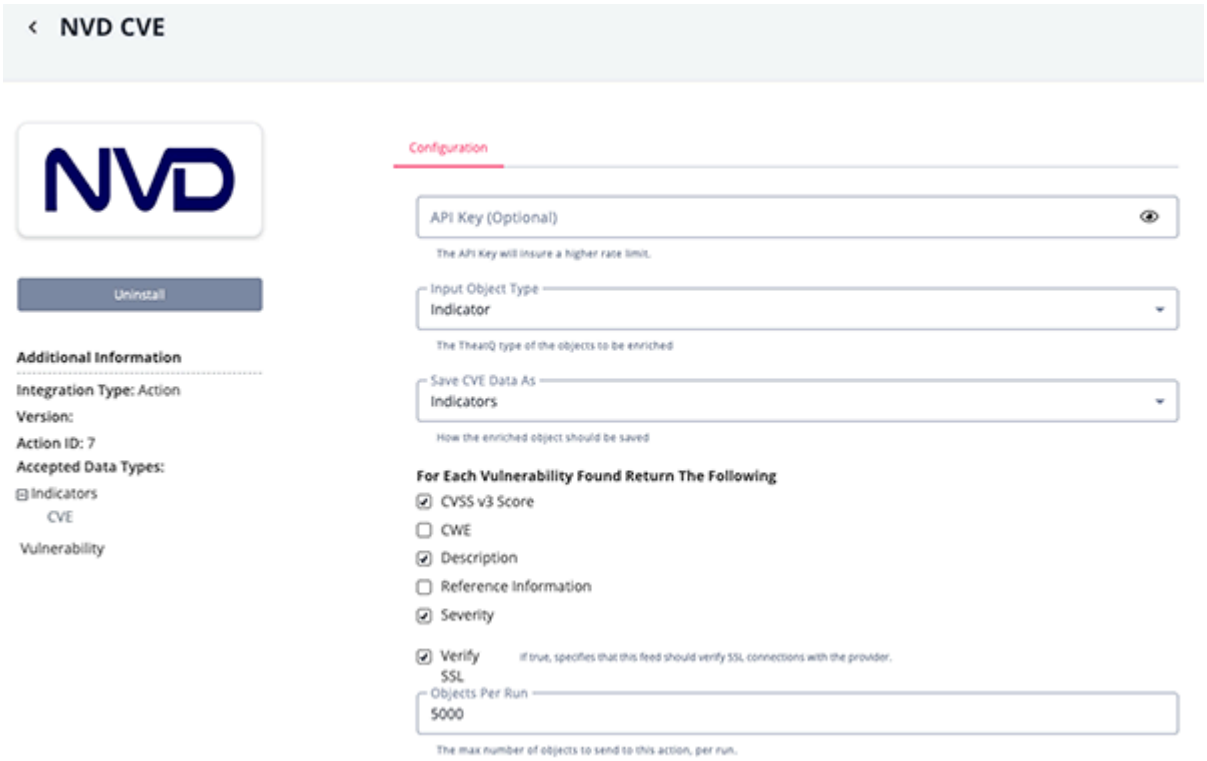
To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Actions** option from the *Category* dropdown (optional).
3. Click on the action entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

> The configurations set on this page will be used as the default settings when inserting this action into a new workflow. Updating the configurations on this page will not update any instances of this action that have already been deployed to a workflow. In that scenario, you must update the action's configurations within the workflow itself.

| PARAMETER | DESCRIPTION |
|---|---|
| **API Key** | Optional - Enter your NVD API Key. Using an API Key will increase your rate limit. |
| **Input Object Type** | Select the type of objects to be enriched. Options include:<br>◦ Indicator<br>◦ Vulnerability |
| **Save CVE Data As** | Select how the enriched objects should be saved. Options include:<br>◦ Indicator<br>◦ Vulnerability |

| PARAMETER | DESCRIPTION |
|---|---|
| **For Each Vulnerability Found Return the Following** | Select the data that will be returned with each vulnerability. Options include:<br>◦ CVSS V3 Score (default)<br>◦ CWE<br>◦ Description (default)<br>◦ Reference Information<br>◦ Severity (default) |
| **Verify SSL** | If enabled, the action will verify SSL connections with the provider. |
| **Objects per Run** | The max number of objects to submit per action. |




5. Review any additional settings, make any changes if needed, and click on **Save**.

# Action Functions

The following action is available with the integration:

| ACTION | DESCRIPTION | OBJECT TYPE | OBJECT SUBTYPE |
|---|---|---|---|
| NVD CVE | Submits CVEs and Vulnerabilities to be enriched. | Indicators, Vulnerabilities | CVE |

# NVD CVE

The NVD CVE action enriches the selected collection of CVE indicators and Vulnerabilities.

> The objects sent to NVD and how the enriched data is saved can be configured in the action's configuration settings.

`GET https://services.nvd.nist.gov/rest/json/cves/2.0?cveId={cve}`

### Sample Response:


```
{
    "resultsPerPage": 1,
    "startIndex": 0,
    "totalResults": 1,
    "format": "NVD_CVE",
    "version": "2.0",
    "timestamp": "2023-04-27T13:17:35.310",
    "vulnerabilities": [
        {
            "cve": {
                "id": "CVE-2002-1949",
                "sourceIdentifier": "cve@mitre.org",
                "published": "2002-12-31T05:00:00.000",
                "lastModified": "2008-09-05T20:31:55.997",
                "vulnStatus": "Analyzed",
                "descriptions": [
                    {
                        "lang": "en",
                        "value": "The Network Attached Storage (NAS) Administration Web Page for Iomega NAS A300U
transmits passwords in cleartext, which allows remote attackers to sniff the administrative password."
                    }
                ],
                "metrics": {
                    "cvssMetricV2": [
                        {
                            "source": "nvd@nist.gov",
                            "type": "Primary",
                            "cvssData": {
                                "version": "2.0",
                                "vectorString": "AV:N/AC:L/Au:N/C:P/I:N/A:N",
                                "accessVector": "NETWORK",
                                "accessComplexity": "LOW",
                                "authentication": "NONE",
                                "confidentialityImpact": "PARTIAL",
                                "integrityImpact": "NONE",
                                "availabilityImpact": "NONE",
                                "baseScore": 5.0
                            },
                            "baseSeverity": "MEDIUM",
                            "exploitabilityScore": 10.0,
                            "impactScore": 2.9,
                            "acInsufInfo": false,
                            "obtainAllPrivilege": false,
```

```
                        "obtainUserPrivilege": false,
                        "obtainOtherPrivilege": false,
                        "userInteractionRequired": false
                    }
                ]
            },
            "weaknesses": [
                {
                    "source": "nvd@nist.gov",
                    "type": "Primary",
                    "description": [
                        {
                            "lang": "en",
                            "value": "NVD-CWE-Other"
                        }
                    ]
                }
            ],
            "configurations": [
                {
                    "nodes": [
                        {
                            "operator": "OR",
                            "negate": false,
                            "cpeMatch": [
                                {
                                    "vulnerable": true,
                                    "criteria": "cpe:2.3:h:iomega:nas:a300u:*:*:*:*:*:*:*",
                                    "matchCriteriaId": "DA964A81-948D-4E38-8991-B72B9302A6D5"
                                }
                            ]
                        }
                    ]
                }
            ],
            "references": [
                {
                    "url": "http://www.securityfocus.com/bid/6092",
                    "source": "cve@mitre.org"
                }
            ]
        }
    }
  ]
}
```


ThreatQuotient provides the following default mapping for this action:

| 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 |

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| .vulnerabilities[].cve.lastModified | Indicator.Attribute / Vulnerability.Attribute | Last Modified | .vulnerabilities[].cve.published | 2023-03-24T20:34:11.990 | Extracted from `.vulnerabilities[].cve.id` |
| .vulnerabilities[].cve.id | Indicator.Attribute / Vulnerability.Attribute | Year | .vulnerabilities[].cve.published | 2018 | N/A |
| .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 |
| .vulnerabilities[].cve.metrics.cvssMetricV31.exploitabilityScore | Indicator.Attribute / Vulnerability.Attribute | CVSSv31 Exploitability Score | .vulnerabilities[].cve.published | 2.8 | If `CVSS v3 Score` option is selected |
| .vulnerabilities[].cve.metrics.cvssMetricV31.cvssData.attackVector | Indicator.Attribute / Vulnerability.Attribute | CVSSv31 Attack Vector | .vulnerabilities[].cve.published | ADJACENT_NETWORK | N/A |
| .vulnerabilities[].cve.metrics.cvssMetricV31.cvssData.attackComplexity | Indicator.Attribute / Vulnerability.Attribute | CVSSv31 Attack Complexity | .vulnerabilities[].cve.published | LOW | N/A |
| .vulnerabilities[].cve.metrics.cvssMetricV31.cvssData.availabilityImpact | Indicator.Attribute / Vulnerability.Attribute | CVSSv31 Availability Impact | .vulnerabilities[].cve.published | HIGH | N/A |
| .vulnerabilities[].cve.metrics.cvssMetricV31.cvssData.baseScore | Indicator.Attribute / Vulnerability.Attribute | CVSSv31 Base Score | .vulnerabilities[].cve.published | 6.5 | If `CVSS v3 Score` |

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| | | | | | option is selected |
| .vulnerabilities[].cve.metrics.cvssMetricV31.cvssData.baseSeverity | Indicator.Attribute / Vulnerability.Attribute | CVSSv31 Base Severity | .vulnerabilities[].cve.published | MEDIUM | If `Severity` option is selected |
| .vulnerabilities[].cve.metrics.cvssMetricV31.cvssData.confidentialityImpact | Indicator.Attribute / Vulnerability.Attribute | CVSSv31 Confidentiality Impact | .vulnerabilities[].cve.published | PARTIAL | N/A |
| .vulnerabilities[].cve.metrics.cvssMetricV31.cvssData.integrityImpact | Indicator.Attribute / Vulnerability.Attribute | CVSSv31 Integrity Impact | .vulnerabilities[].cve.published | HIGH | N/A |
| .vulnerabilities[].cve.metrics.cvssMetricV31.cvssData.privilegesRequired | Indicator.Attribute / Vulnerability.Attribute | CVSSv31 Privileges Required | .vulnerabilities[].cve.published | NONE | N/A |
| .vulnerabilities[].cve.metrics.cvssMetricV31.cvssData.scope | Indicator.Attribute / Vulnerability.Attribute | CVSSv31 Scope | .vulnerabilities[].cve.published | UNCHANGED | N/A |
| .vulnerabilities[].cve.metrics.cvssMetricV31.cvssData.userInteraction | Indicator.Attribute / Vulnerability.Attribute | CVSSv31 User Interaction | .vulnerabilities[].cve.published | REQUIRED | N/A |
| .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 | N/A |
| .vulnerabilities[].cve.metrics.cvssMetricV31.cvssData.version | Indicator.Attribute / Vulnerability.Attribute | CVSSv31 Version | .vulnerabilities[].cve.published | 3.1 | N/A |
| .vulnerabilities[].cve.metrics.cvssMetricV30.impactScore | Indicator.Attribute / Vulnerability.Attribute | CVSSv30 Impact Score | .vulnerabilities[].cve.published | 5.9 | If `CVSS v3 Score` option is selected |
| .vulnerabilities[].cve.metrics.cvssMetricV30.exploitabilityScore | Indicator.Attribute / Vulnerability.Attribute | CVSSv30 Exploitability Score | .vulnerabilities[].cve.published | 2.8 | If `CVSS v3 Score` option is selected |
| .vulnerabilities[].cve.metrics.cvssMetricV30.cvssData.attackVector | Indicator.Attribute / Vulnerability.Attribute | CVSSv30 Attack Vector | .vulnerabilities[].cve.published | ADJACENT_NETWORK | N/A |
| .vulnerabilities[].cve.metrics.cvssMetricV30.cvssData.attackComplexity | Indicator.Attribute / Vulnerability.Attribute | CVSSv30 Attack Complexity | .vulnerabilities[].cve.published | LOW | N/A |
| .vulnerabilities[].cve.metrics.cvssMetricV30.cvssData.availabilityImpact | Indicator.Attribute / Vulnerability.Attribute | CVSSv30 Availability Impact | .vulnerabilities[].cve.published | HIGH | N/A |
| .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 |
| .vulnerabilities[].cve.metrics.cvssMetricV30.cvssData.baseSeverity | Indicator.Attribute / Vulnerability.Attribute | CVSSv30 Base Severity | .vulnerabilities[].cve.published | MEDIUM | If `Severity` option is selected |

| 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 | N/A |
| .vulnerabilities[].cve.metrics.cvssMetricV30.cvssData.integrityImpact | Indicator.Attribute / Vulnerability.Attribute | CVSSv30 Integrity Impact | .vulnerabilities[].cve.published | HIGH | N/A |
| .vulnerabilities[].cve.metrics.cvssMetricV30.cvssData.privilegesRequired | Indicator.Attribute / Vulnerability.Attribute | CVSSv30 Privileges Required | .vulnerabilities[].cve.published | NONE | N/A |
| .vulnerabilities[].cve.metrics.cvssMetricV30.cvssData.scope | Indicator.Attribute / Vulnerability.Attribute | CVSSv30 Scope | .vulnerabilities[].cve.published | UNCHANGED | N/A |
| .vulnerabilities[].cve.metrics.cvssMetricV30.cvssData.userInteraction | Indicator.Attribute / Vulnerability.Attribute | CVSSv30 User Interaction | .vulnerabilities[].cve.published | REQUIRED | N/A |
| .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 | N/A |
| .vulnerabilities[].cve.metrics.cvssMetricV30.cvssData.version | Indicator.Attribute / Vulnerability.Attribute | CVSSv30 Version | .vulnerabilities[].cve.published | 3.0 | N/A |
| .vulnerabilities[].cve.metrics.cvssMetricV2.impactScore | Indicator.Attribute / Vulnerability.Attribute | CVSSv2 Impact Score | .vulnerabilities[].cve.published | 5.9 | N/A |
| .vulnerabilities[].cve.metrics.cvssMetricV2.exploitabilityScore | Indicator.Attribute / Vulnerability.Attribute | CVSSv2 Exploitability Score | .vulnerabilities[].cve.published | 2.8 | N/A |
| .vulnerabilities[].cve.metrics.cvssMetricV2.acInsufInfo | Indicator.Attribute / Vulnerability.Attribute | CVSSv2 AC Insuf Info | .vulnerabilities[].cve.published | true | N/A |
| .vulnerabilities[].cve.metrics.cvssMetricV2.obtainOtherPrivilege | Indicator.Attribute / Vulnerability.Attribute | CVSSv2 Obtain Other Privilege | .vulnerabilities[].cve.published | false | N/A |
| .vulnerabilities[].cve.metrics.cvssMetricV2.obtainUserPrivilege | Indicator.Attribute / Vulnerability.Attribute | CVSSv2 Obtain User Privilege | .vulnerabilities[].cve.published | false | N/A |
| .vulnerabilities[].cve.metrics.cvssMetricV2.obtainAllPrivilege | Indicator.Attribute / Vulnerability.Attribute | CVSSv2 Obtain All Privilege | .vulnerabilities[].cve.published | false | N/A |
| .vulnerabilities[].cve.metrics.cvssMetricV2.userInteractionRequired | Indicator.Attribute / Vulnerability.Attribute | CVSSv2 User Interaction Required | .vulnerabilities[].cve.published | false | N/A |
| .vulnerabilities[].cve.metrics.cvssMetricV2.baseSeverity | Indicator.Attribute / Vulnerability.Attribute | CVSSv2 Base Severity | .vulnerabilities[].cve.published | HIGH | N/A |
| .vulnerabilities[].cve.metrics.cvssMetricV2.cvssData.accessComplexity | Indicator.Attribute / Vulnerability.Attribute | CVSSv2 Access Complexity | .vulnerabilities[].cve.published | LOW | N/A |
| .vulnerabilities[].cve.metrics.cvssMetricV2.cvssData.availabilityImpact | Indicator.Attribute / Vulnerability.Attribute | CVSSv2 Availability Impact | .vulnerabilities[].cve.published | HIGH | N/A |

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| .vulnerabilities[].cve.metrics.cvssMetricV2.cvssData.accessVector | Indicator.Attribute / Vulnerability.Attribute | CVSSv2 Access Vector | .vulnerabilities[].cve.published | NETWORK | N/A |
| .vulnerabilities[].cve.metrics.cvssMetricV2.cvssData.authentication | Indicator.Attribute / Vulnerability.Attribute | CVSSv2 Authentication | .vulnerabilities[].cve.published | SINGLE | N/A |
| .vulnerabilities[].cve.metrics.cvssMetricV2.cvssData.baseScore | Indicator.Attribute / Vulnerability.Attribute | CVSSv2 Base Score | .vulnerabilities[].cve.published | 6.5 | N/A |
| .vulnerabilities[].cve.metrics.cvssMetricV2.cvssData.confidentialityImpact | Indicator.Attribute / Vulnerability.Attribute | CVSSv2 Confidentiality Impact | .vulnerabilities[].cve.published | PARTIAL | N/A |
| .vulnerabilities[].cve.metrics.cvssMetricV2.cvssData.integrityImpact | Indicator.Attribute / Vulnerability.Attribute | CVSSv2 Integrity Impact | .vulnerabilities[].cve.published | HIGH | N/A |
| .vulnerabilities[].cve.metrics.cvssMetricV2.cvssData.vectorString | Indicator.Attribute / Vulnerability.Attribute | CVSSv2 Vector String | .vulnerabilities[].cve.published | CVSS:3.0/AV:A/AC:L/PR:N/C:N/I:H/A:H | N/A |
| .vulnerabilities[].cve.metrics.cvssMetricV2.cvssData.version | Indicator.Attribute / Vulnerability.Attribute | CVSSv2 Version | .vulnerabilities[].cve.published | 2.0 | N/A |

# Enriched Data

Object counts and action runtime are supplied as generalities only - objects returned by a provider can differ based on credential configurations and action runtime may vary based on system resources and load.

| METRIC | RESULT |
|---|---|
| Run Time | 1 minute |
| Indicators | 1 |
| Indicator Attributes | 22 |

# Known Issues / Limitations

- A 7-second delay has been applied to the action to avoid the NIST rate limit.  This will prevent the NIST firewall rules rejecting requests.  You can use the optional API Key configuration option to increase the rate limit.

# Change Log

- **Version 1.0.2**
  - Added the option to call the API using an API Key.  This will allow you to increase your rate limit.
  - Added a new optional configuration parameter: API Key.
  - Increased the default Number of Objects Per Run to 5000.
- **Version 1.0.1**
  - Added support for Vulnerabilities to be sent for enrichment.
  - Added three new configuration fields: **Input Object Type**, **Save CVE Data As**, and **For Each Vulnerability Found Return the Following**.
- **Version 1.0.0**
  - Initial release