ThreatQuotient

Intel 471 Vulnerability Reports Feed Implementation Guide

Version 1.1.0

Monday, August 3, 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, August 3, 2020

Contents

Versioning

- Current integration version `1.1.0`
- Supported on ThreatQ versions >= `4.28.0`

Introduction

The Intel 471 Vulnerability Reports feed ingests threat intelligence data from the following endpoint:

- https://api.intel471.com/v1/cve/reports

Notes:

- Uses basic HTTP authentication based on email address and API key.

  > ThreatQuotient does not issue third-party credentials. Contact Intel 471 for the required credentials.

- Time constrained data fetching is possible.

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 **Intel 471 Vulnerability Reports** 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 **Commercial** 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 **Commercial** tab.
3. Click on the **Feed Settings** link for the feed.
4. Under the **Connection** tab, enter the following configuration parameters:

Parameter	Description
Email Address	The vendor-supplied email address.
API Key	The vendor-supplied API Key.
Save CVE Data as	Select whether to ingest CVEs as ThreatQ Vulnerability objects, Indicator objects, or both. The Indicators option is selected by default.

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

ThreatQ Mapping

The Intel 471 Vulnerability Reports feed provides an API that users can use to extract data in JSON format.

JSON Response Sample 1


```
{
   "cveReportsTotalCount":1,
   "cveReports":[
      {
         "data":{
            "cve_report":{
               "risk_level":"high",
               "name":"CVE-2018-20250",
               "activity_location":{
                  "location_opensource":true,
                  "location_underground":true
               },
               "vendor_name":"RARLab",
               "exploit_status":{
                  "available":true,
                  "productized":true
               },
               "titan_links":[
                  {
                     "title":"WinRAR CVE-2018-20250 Exploit |
Spread FAST",
                     "url":"https://titan.intel471.com/post_
```

```
thread/4c30f13ded0db96f789f2eeaf3d45020?post_uid-
d=6a29bf81f82bda975124aeb32a7074ba"
                  },
                  {
Table Row Outside Table:  "title":"WINRAR EXPLOIT!! CVE 2018 20250
Table Cell Outside Table:  FAST SPREADING

500 MILLION USERS EXPOSED",
                     "url":"https://titan.intel471.com/post_
thread/61bead81b9eee36fde5add081a3425f9?post_uid-
d=c63793e2625349e8f741ebc01f85f151"
                  },
                  {
                     "title":"Критическая уязвимость в WinRAR
ставит под угрозу более 500 млн пользователей",
                     "url":"https://titan.intel471.com/post_
thread/b81726a9d01dcb4e5734dda1f666f8b6?post_uid-
d=15c55952778dc4103bc04df8200c9ebc"
                  }
               ],
               "patch_status":"available",
               "poc":"observed",
               "counter_measures":"The impacted vendor
released patching information for impacted products and cor-
responding versions. The vendor likely addressed the vul-
nerability in a version update.",
               "interest_level":{
                  "disclosed_publicly":true,
                  "researched_publicly":true,
                  "exploit_sought":true
```

```
            },
            "product_name":"WinRAR",
            "cve_type":"Path traversal",
            "poc_links":[
               {
                  "title":"Exploit status ",
                  "url":" https://www.exploit-db.-
com/exploits/46756"
               }
            ],
            "detection":"available",
            "cvss_score":{
               "v2":6.8,
               "v3":7.8
            },
            "underground_activity_summary":"Intel 471 did
not observe weaponization or productization of CVE-2018-20250
in the underground. Intel 471 observed several actors post
links to open-source articles and a PoC for CVE-2018-20250.",
            "cve_status":"status_historical",
            "underground_activity":"observed",
            "cpe":{
               "cve_data_version":"4.0",
               "nodes":[
                  {
                     "operator":"OR",
                     "cpe_match":[
                        {
                           "vulnerable":true,
```

```
                              "cpe23Uri":"cpe:2.3:a:rar-
lab:winrar:*:*:*:*:*:*:*:*",
                              "versionEndIncluding":"5.61"
                           }
                        ]
                     }
                  ]
               },
               "summary":"CVE-2018-20250 is a path traversal
vulnerability impacting the WinRAR data compression tool’s
archive file format (ACE). A proof of concept (PoC) was
observed publicly or in the underground."
            }
         },
         "last_updated":1570813574273,
         "uid":"daa5170f9d73629908d8a9170b6c3066",
         "classification":{
            "intel_requirements":[
               "2.1.2.2",
               "2.2.1"
            ]
         },
         "activity":{
            "first":1570556602000,
            "last":1570556602000
         }
      }
   ]
}
```

JSON Response Sample 2


```
{
   "cveReportsTotalCount":1,
   "cveReports":[
      {
         "data":{
            "cve_report":{
               "risk_level":"high",
               "name":"CVE-2018-20250",
               "activity_location":{
                  "location_opensource":true,
                  "location_underground":true
               },
               "vendor_name":"RARLab",
               "exploit_status":{
                  "available":true,
                  "productized":true
               },
               "titan_links":[
                  {
                     "title":"WinRAR CVE-2018-20250 Exploit |
Spread FAST",
                     "url":"https://titan.intel471.com/post_
thread/4c30f13ded0db96f789f2eeaf3d45020?post_uid-
d=6a29bf81f82bda975124aeb32a7074ba"
                  },
                  {
Table Row Outside Table:  "title":"WINRAR EXPLOIT!! CVE 2018 20250
Table Cell Outside Table:  FAST SPREADING
```

```
500 MILLION USERS EXPOSED",
                    "url":"https://titan.intel471.com/post_
thread/61bead81b9eee36fde5add081a3425f9?post_uid-
d=c63793e2625349e8f741ebc01f85f151"
                },
                {
                    "title":"Критическая уязвимость в WinRAR
ставит под угрозу более 500 млн пользователей",
                    "url":"https://titan.intel471.com/post_
thread/b81726a9d01dcb4e5734dda1f666f8b6?post_uid-
d=15c55952778dc4103bc04df8200c9ebc"
                }
            ],
            "patch_status":"available",
            "poc":"observed",
            "counter_measures":"The impacted vendor
released patching information for impacted products and cor-
responding versions. The vendor likely addressed the vul-
nerability in a version update.",
            "interest_level":{
                "disclosed_publicly":true,
                "researched_publicly":true,
                "exploit_sought":true
            },
            "product_name":"WinRAR",
            "cve_type":"Path traversal",
            "poc_links":[
                {
                    "title":"Exploit status ",
```

```
                    "url":" https://www.exploit-db.-
com/exploits/46756"
                }
            ],
            "detection":"available",
            "cvss_score":{
               "v2":6.8,
               "v3":7.8
            },
            "underground_activity_summary":"Intel 471 did
not observe weaponization or productization of CVE-2018-20250
in the underground. Intel 471 observed several actors post
links to open-source articles and a PoC for CVE-2018-20250.",
            "cve_status":"status_historical",
            "underground_activity":"observed",
            "cpe":{
               "cve_data_version":"4.0",
               "nodes":[
                  {
                    "operator": "OR"
                    "children": [
                       {
                          "operator":"OR",
                          "cpe_match":[
                             {
                                "vulnerable":true,
                                "cpe23Uri":"cpe:2.3:a:rar-
lab:winrar:*:*:*:*:*:*:*:*",
                                "versionEndIncluding":"5.61"
```

```
                                    }
                                ]
                            }
                        ]
                    }
                ]
            },
            "summary":"CVE-2018-20250 is a path traversal
vulnerability impacting the WinRAR data compression tool’s
archive file format (ACE). A proof of concept (PoC) was
observed publicly or in the underground."
         }
      },
      "last_updated":1570813574273,
      "uid":"daa5170f9d73629908d8a9170b6c3066",
      "classification":{
         "intel_requirements":[
            "2.1.2.2",
            "2.2.1"
         ]
      },
      "activity":{
         "first":1570556602000,
         "last":1570556602000
      }
   }
]
}
```

The mapping table is below.

Feed Data	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples
.cveReports[].data.uid	vul- ner- ability.attribute/indicator.attribute	Report UID	.cveReports [].data.cve_ report.activ- ity.first	daa5170f9d73629908d8a9170b6c3- 066
.cveReports[].data.cve_ report.name	vulnerability.value/indicator.value	N/A	.cveReports [].data.cve_ report.activ- ity.first	CVE-2018-20250
.cveReports[].data.cve_ report.risk_level	vul- ner- ability.attribute/indicator.attribute	Risk Level	.cveReports [].data.cve_ report.activ- ity.first	low
.cveReports[].data.cve_ report.cve_type	vul- ner-	CVE Type	.cveReports [].data.cve_	Path traversal

Feed Data	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples
	ability.attribute/indicator.attribute		report.activ-ity.first	
.cveReports[].data.cve_report.vendor_name	vul-ner-ability.attribute/indicator.attribute	Vendor Name	.cveReports[].data.cve_report.activ-ity.first	Vendor Name
.cveReports[].data.cve_report.product_name	vul-ner-ability.attribute/indicator.attribute	Product Name	.cveReports[].data.cve_report.activ-ity.first	WinRAR
.cveReports[].data.cve_report.detection	vul-ner-ability.attribute/indicator.attribute	Detection	.cveReports[].data.cve_report.activ-ity.first	available
.cveReports[].data.cve_report.undeground_activity_	vul-ner-	Under-ground Activ-	.cveReports[].data.cve_	Intel 471 did not observe weapon-ization

Feed Data	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples
summary	ability.attribute/indicator.attribute	ity Summary	report.activ-ity.first	
.cveReports[].data.cve_report.cve_status	vul-ner-ability.attribute/indicator.attribute	CVE Status	.cveReports[].data.cve_report.activ-ity.first	status_historical
.cveReports[].data.cve_report.interest_level.dis-closed_publicly	vul-ner-ability.attribute/indicator.attribute	Disclosed Publicly	.cveReports[].data.cve_report.activ-ity.first	true
.cveReports[].data.cve_report.interest_level.re-searched_publicly	vul-ner-ability.attribute/indicator.attribute	Researched Publicly	.cveReports[].data.cve_report.activ-ity.first	true
.cveReports[].data.cve_report.interest_level.exploit_	vul-ner-	Exploit Sought	.cveReports[].data.cve_	true

Feed Data	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples
sought	ability.attribute/indicator.attribute		report.activity.first	
.cveReports[].data.cve_report.activity_location.location_opensource	vulnerability.attribute/indicator.attribute	Activity Location Opensource	.cveReports[].data.cve_report.activity.first	true
.cveReports[].data.cve_report.activity_location.location_underground	vulnerability.attribute/indicator.attribute	Activity Location Underground	.cveReports[].data.cve_report.activity.first	true
.cveReports[].data.cve_report.activity_location.location_private	vulnerability.attribute/indicator.attribute	Activity Location Private	.cveReports[].data.cve_report.activity.first	true
.cveReports[].data.cve_report.exploit_status.avail-	vulner-	Exploit Status Avail-	.cveReports[].data.cve_	true

Feed Data	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples
able	ability.attribute/indicator.attribute	able	report.activ-ity.first	
.cveReports[].data.cve_report.exploit_status.weaponized	vul-ner-ability.attribute/indicator.attribute	Exploit Status Weaponized	.cveReports[].data.cve_report.activ-ity.first	true
.cveReports[].data.cve_report.exploit_status.-productized	vul-ner-ability.attribute/indicator.attribute	Exploit Status Pro-ductized	.cveReports[].data.cve_report.activ-ity.first	true
.cveReports[].data.cve_report.exploit_status.not_observed	vul-ner-ability.attribute/indicator.attribute	Exploit Status Not Observed	.cveReports[].data.cve_report.activ-ity.first	true
.cveReports[].data.cve_report.cvss_score.v2	vul-ner-	CVSS Score V2	.cveReports[].data.cve_	6.8

Feed Data	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples
	ability.attribute/indicator.attribute		report.activ-ity.first	
.cveReports[].data.cve_report.cvss_score.v3	vul-ner-ability.attribute/indicator.attribute	CVSS Score v3	.cveReports[].data.cve_report.activ-ity.first	7.3
.cveReports[].data.cve_report.patch_status	vul-ner-ability.attribute/indicator.attribute	Patch Status	.cveReports[].data.cve_report.activ-ity.first	available
.cveReports[].data.cve_report.underground_activity	vul-ner-ability.attribute/indicator.attribute	Under-ground activ-ity	.cveReports[].data.cve_report.activ-ity.first	observed
.cveReports[].data.cve_report.counter_measures	vul-ner-	POC Link Counter	.cveReports[].data.cve_	The impact vendor released patch-ing information for impacted product

Feed Data	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples
	ability.attribute/indicator.attribute	Measures	report.activity.first	
.cveReports[].data.cve_report.summary	vulnerability.attribute/indicator.attribute	Summary	.cveReports[].data.cve_report.activity.first	CVE-2019-5786 is a use after free vulnerability impacting Google Chrome versions
.cveReports[].data.cve_report.titan_links.title, .cveReports[].data.cve_report.titan_links.url, .cveReports[].data.cve_report.title_links.poc	vulnerability.attribute/indicator.attribute	Titan Link Title, Titan Link URL, Titan Links POC	.cveReports[].data.cve_report.activity.first	В Google Chrome обнаружена критическая 0Day, http://some.com
.cveReports[].data.cve_report.titan_links.title, .cveReports[].data.cve_report.titan_links.url	vulnerability.attribute/indicator.attribute	Titan Link Title, Titan Link URL	.cveReports[].data.cve_report.activity.first	

Feed Data	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples
.cveReports[].data.cve_report.poc_links.title, .cveReports[].data.cve_report.poc_links.url	vulnerability.attribute/indicator.attribute	POC Link Title, POC Link URL	.cveReports[].data.cve_report.activity.first	Chromium proof of concept
.cveReports[].data.cve_report.counter_measures_links.title, .cveReports[].data.cve_report.counter_measures_links.url	vulnerability.attribute/indicator.attribute	Counter Measures Title, Counter Measures URL	.cveReports[].data.cve_report.activity.first	
.cveReports[].data.cve_report.patch_links.title, .cveReports[].data.cve_report.patch_links.url	vulnerability.attribute/indicator.attribute	Patch Link Title, Patch Link URL	.cveReports[].data.cve_report.activity.first	Chrome release security fix
.cveReports[].data.cve_report.classification.intel_	vulner-	Intel Require-	.cveReports[].data.cve_	["2.1.2.1", "2.1.2.2"]

Feed Data	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples
requirements	ability.attribute/indicator.attribute	ments	report.activ-ity.first	
.cveReports[].data.cve_report.last_updated	vul-ner-ability.attribute/indicator.attribute	Last Updated At	.cveReports[].data.cve_report.activ-ity.first	2000-01-01 21:21:21
.cveReports[].data.cve_report.activity.first	vul-ner-ability.attribute/indicator.attribute	Created At	.cveReports[].data.cve_report.activ-ity.first	2000-01-01 21:21:21
.cveReports[].data.cve_report.activity.last	vul-ner-ability.attribute/indicator.attribute	Last Activity At	.cveReports[].data.cve_report.activ-ity.first	2000-01-01 21:21:21
.cveReports[].data.cve_	vul-ner-	Cpe23Uri, Vulnerability	.cveReports[].data.cve_	cpe:2.3:a:schben:adive:*:*:*:*:*:*:*:*", true

Feed Data	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples
report.cpe.nodes.cpe_match.cpe23Uri, .cveReports[].data.cve_report.cpe.nodes.cpe_match.vulnerable	ability.attribute/indicator.attribute		report.activity.first	
.cveReports[].data.cve_report.cpe.nodes.children.cpe_match.cpe23Uri, .cveReports[].data.cve_report.cpe.nodes.children.cpe_match.vulnerable	vulnerability.attribute/indicator.attribute	Cpe23Uri, Vulnerability	.cveReports[].data.cve_report.activity.first	cpe:2.3:a:schben:adive:::::::", true

Average Feed Run

Metric	Result
Run Time	10 Minutes
Indicators	569
Indicator Attributes	26,844
Vulnerabilities	759
Vulnerability Attributes	26,844

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 1.1.0**
  - Added 'Save CVE Data As' user configuration parameter.
- **Version 1.0.0**
  - Initial release.