ThreatQuotient

Intel 471 Vulnerability Reports Feed Implementation Guide

Version 1.0.0

Tuesday, December 10, 2019

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, December 10, 2019

Contents

Versioning

- Current integration version `1.0.0`
- 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.

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	Examples
cveReports.uid	vulnerability.attribute	Report UID	daa5170f9d73629908d8a9170b6c3066
cveReports.cve_report.name	vulnerability.value	N/A	CVE-2018-20250
cveReports.cve_report.risk_level	vulnerability.attribute	Risk Level	low
cveReports.cve_report.cve_type	vulnerability.attribute	CVE Type	Path traversal
cveReports.cve_report.vendor_name	vulnerability.attribute	Vendor Name	Vendor Name
cveReports.cve_report.product_name	vulnerability.attribute	Product Name	WinRAR
cveReports.cve_report.detection	vulnerability.attribute	Detection	available
cveReports.cve_report.undeground_activity_summary	vulnerability.attribute	Underground Activity Summary	Intel 471 did not observe weaponization
cveReports.cve_report.cve_status	vulnerability.attribute	CVE Status	status_historical
cveReports.cve_report.interest_level.disclosed_publicly	vulnerability.attribute	Disclosed Publicly	true

Feed Data	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples
cveReports.cve_report.interest_level.re-searched_publicly	vulnerability.attribute	Researched Publicly	true
cveReports.cve_report.interest_level.exploit_sought	vulnerability.attribute	Exploit Sought	true
cveReports.cve_report.activity_location.location_opensource	vulnerability.attribute	Activity Location Opensource	true
cveReports.cve_report.activity_location.location_underground	vulnerability.attribute	Activity Location Underground	true
cveReports.cve_report.activity_location.location_private	vulnerability.attribute	Activity Location Private	true
cveReports.cve_report.exploit_status.available	vulnerability.attribute	Exploit Status Available	true
cveReports.cve_report.exploit_status.weapon-ized	vulnerability.attribute	Exploit Status Weaponized	true
cveReports.cve_report.exploit_status.productized	vulnerability.attribute	Exploit Status	true

Feed Data	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples
		Productized	
cveReports.cve_report.exploit_status.not_observed	vulnerability.attribute	Exploit Status Not Observed	true
cveReports.cve_report.cvss_score.v2	vulnerability.attribute	CVSS Score V2	6.8
cveReports.cve_report.cvss_score.v3	vulnerability.attribute	CVSS Score v3	7.3
cveReports.cve_report.patch_status	vulnerability.attribute	Patch Status	available
cveReports.cve_report.underground_activity	vulnerability.attribute	Underground activity	observed
cveReports.cve_report.counter_measures	vulnerability.attribute	POC Link Counter Meas-ures	The impact vendor released patching information for impacted product
cveReports.cve_report.summary	vulnerability.attribute	Summary	CVE-2019-5786 is a use after free vul-nerability impacting Google Chrome ver-sions
cveReports.cve_report.titan_links.title, cveRe-	vulnerability.attribute	Titan Link Title,	B Google Chrome обнаружена

Feed Data	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples
ports.cve_report.titan_links.url, cveReports.cve_report.title_links.poc		Titan Link Url, Titan Links POC	критическая 0Day, http://some.com,
cveReports.cve_report.titan_links.title, cveReports.cve_report.titan_links.url	vulnerability.attribute	Titan Link Title, Titan Link Url	Chromium proof of concept
cveReports.cve_report.poc_links.title, cveReports.cve_report.poc_links.url	vulnerability.attribute	POC Link Title, POC Link Url	
cveReports.cve_report.counter_measures_links.title, cveReports.cve_report.counter_measures_links.url	vulnerability.attribute	Counter Measures Title, Counter Measures Url	Chrome release security fix
cveReports.cve_report.patch_links.title, cveReports.cve_report.patch_links.url	vulnerability.attribute	Patch Link Title, Patch Link Url	
cveReports.cve_report.classification.intel_requirements	vulnerability.attribute	Intel Requirements	["2.1.2.1", "2.1.2.2"]
cveReports.cve_report.last_updated	vulnerability.attribute	Last Updated At	2000-01-01 21:21:21

Feed Data	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples
cveReports.cve_report.activity.first	vulnerability.attribute	Created At	2000-01-01 21:21:21
cveReports.cve_report.activity.first	vulnerability.published_at	N/A	2000-01-01 21:21:21
cveReports.cve_report.activity.last	vulnerability.attribute	Last Activity At	2000-01-01 21:21:21
cveReports.cve_report.cpe.nodes.cpe_match.cpe23Uri, cveReports.cve_report.cpe.nodes.cpe_match.vulnerable	vulnerability.attribute	Cpe23Uri, Vulnerability	cpe:2.3:a:schben:adive:*:*:*:*:*:*:*:*", true
cveReports.cve_report.cpe.nodes.children.cpe_match.cpe23Uri, cveReports.cve_report.cpe.nodes.children.cpe_match.vulnerable	vulnerability.attribute	Cpe23Uri, Vulnerability	cpe:2.3:a:schben:adive:*:*:*:*:*:*:*:*", true