ThreatQuotient

Feedly CDF Guide

Version 1.0.0

April 12, 2022

ThreatQuotient
11400 Commerce Park Dr., Suite 200
Reston, VA 20191

Not Supported

Contents

Support 4
Versioning 5
Introduction 6
Installation 7
Configuration 8
ThreatQ Mapping 10
    Feedly Ingest (Feed) 10
Average Feed Run 15
Known Issues / Limitations 16
Change Log 17

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 **Not Supported**.

Integrations, apps, and add-ons designated as **Not Supported** are not supported by ThreatQuotient's Customer Support team.

While you can report issues to ThreatQ's Customer Support team regarding the integration/app/add-on, you are solely responsible for ensuring proper functionality and version compatibility of Not Supported designations with the applicable ThreatQuotient software.

If unresolvable functional or compatibility issues are encountered, you may be required to uninstall the integration/app/add-on from your ThreatQuotient environment in order for ThreatQuotient to fulfill support obligations.

> ⚠ For ThreatQuotient Hosted instance customers, the Service Level Commitment and Service Level Credit in the ThreatQuotient Service Level Schedule will not apply to issues caused by Not Supported integrations/apps/add-ons.

Versioning

- Current integration version: `1.0.0`
- Compatible with ThreatQ versions >= `4.35.0`

Introduction

The Feedly integration for ThreatQ allows a user to ingest feeds as reports and related objects from Team feeds on Feedly.

> You cannot pull from a Feedly Personal feed.

The CDF includes the following feed:

- **Feedly Ingest** - ingests reports and other related objects from Feedly.

The integration ingests the following system object types:

- Attack Patterns
- Adversaries
- Identities
- Indicators
  - Indicator Attributes
- Malware
- Reports
  - Report Attributes
- Vulnerabilities

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 integration file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration 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 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.
6. If prompted, select the individual feeds to install and click **Install**. The feed will be added to the integrations page.

You will still need to configure and then enable the integration.

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 **Commercial** option from the *Category* dropdown (optional).

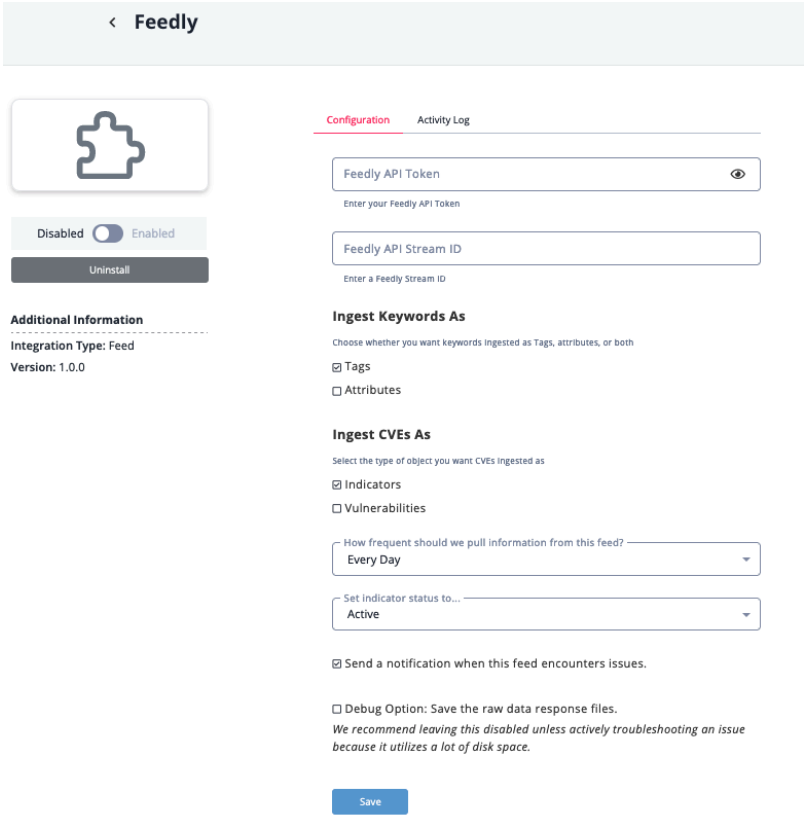
   > If you are installing the integration for the first time, it will be located under the **Disabled** tab.

3. Click on the integration to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Feedly API Token	Your Feedly API Token.
Feedly API Stream ID	Your Feedly Stream ID.
Ingest CVEs As:	Select the type of objects CVEs should be ingested as. Options include: ◦ Indicators (default) ◦ Vulnerabilities - Review the Known Issues / Limitations chapter if using this option. > You have the option of selecting both types.
Ingest Keywords As:	Select the type of object Keywords should be ingested as. Options include: ◦ Tags (default) ◦ Attributes

PARAMETER	DESCRIPTION

> You have the option of selecting both types.



5. Review the **Settings** configuration, make any changes if needed, and click on **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable it.

ThreatQ Mapping

ThreatQuotient provides the following mapping for the Feedly CDF.

Feedly Ingest (Feed)

The Feedly Ingest feed ingests CVE's as indicators or vulnerabilities.

```
GET https://cloud.feedly.com/v3/streams/contents
```

Sample Response


```
{
  "continuation": "17eb965fd82:8f60c7:26e2bd2e",
  "id": "enterprise/threatquotient/category/4b1e06a8-b4de-4e74-9593-ac879d1d3d23",
  "items": [
  {
      "alternate": [
          {
              "href": "https://packetstormsecurity.com/files/165814/wpcfct102-xssaccess.txt",
              "type": "text/html"
          }
      ],
      "canonicalUrl": "https://packetstormsecurity.com/files/165814/wpcfct102-xssaccess.txt",
      "categories": [
          {
              "id": "enterprise/threatquotient/category/4b1e06a8-b4de-4e74-9593-ac879d1d3d23",
              "label": "Threat Intel"
          }
      ],
      "commonTopics": [
          {
              "id": "nlp/f/topic/2440",
              "label": "Vulnerabilities",
              "salienceLevel": "about",
              "score": 1.0,
              "type": "topic"
          },
          {
              "id": "nlp/f/topic/3003",
              "label": "Cyber Security",
              "salienceLevel": "about",
              "score": 1.0,
              "type": "topic"
          }
      ],
      "crawled": 1643826412301,
      "entities": [
          {
              "id": "vulnerability/m/entity/CVE-2021-24247",
              "label": "CVE-2021-24247",
              "mentions": [
```

```
                {
                    "text": "CVE-2021-24247"
                }
            ],
            "vulnerabilityInfo": {
                "cvssScore": 5.4,
                "description": "The Contact Form Check Tester WordPress plugin through 1.0.2 settings are visible
to all registered users in the dashboard and are lacking any sanitisation. As a result, any registered user, such as
subscriber, can leave an XSS payload in the plugin settings, which will be triggered by any user visiting them, and
could allow for privilege escalation. The vendor decided to close the plugin.",
                "hasExploit": true,
                "hasPatch": false
            }
        }
    ],
    "estimatedCVSS": {
        "category": "HIGH"
    },
    "fingerprint": "b5dfd074",
    "fullContent": "<!DOCTYPE html PUBLIC \"-//W3C//DTD HTML 4.0 Transitional//EN\" \"http://www.w3.org/TR/REC-
html40/loose.dtd\">\n<html><body><div><div><div id=\"m\">\n    \n\n    \n    \n    \n    \n    <p></p><h1>WordPress
Contact Form Check Tester 1.0.2 XSS / Access Control</h1>\n<dl id=\"F165814\"><dt><a href=\"https://
packetstormsecurity.com/files/download/165814/wpcfct102-xssaccess.txt\" title=\"Size: 0.7 KB\"><strong>WordPress
Contact Form Check Tester 1.0.2 XSS / Access Control</strong></a></dt>\n<dd>Posted <a href=\"https://
packetstormsecurity.com/files/date/2022-02-02/\" title=\"16:49:09 UTC\">Feb  2, 2022</a></dd>\n<dd>Authored by <a
href=\"https://packetstormsecurity.com/files/author/13412/\">0xB9</a></dd>\n<dd><p>WordPress Contact Form Check
Tester plugin version 1.0.2 suffers from broken access control and cross site scripting vulnerabilities.</p></
dd>\n<dd><span>tags</span> | <a href=\"https://packetstormsecurity.com/files/tags/exploit\">exploit</a>, <a
href=\"https://packetstormsecurity.com/files/tags/vulnerability\">vulnerability</a>, <a href=\"https://
packetstormsecurity.com/files/tags/xss\">xss</a></dd>\n<dd><span>advisories</span> | <a href=\"https://
packetstormsecurity.com/files/cve/CVE-2021-24247\">CVE-2021-24247</a></dd>\n<dd><span>MD5</span> |
<code>6571a974217db95c175bd945e2b0d575</code></dd>\n<dd><a href=\"https://packetstormsecurity.com/files/download/
165814/wpcfct102-xssaccess.txt\" title=\"Size: 0.7 KB\" rel=\"nofollow\">Download</a>  | <a href=\"https://
packetstormsecurity.com/files/favorite/165814/\" rel=\"nofollow\">Favorite</a> | <a href=\"https://
packetstormsecurity.com/files/165814/WordPress-Contact-Form-Check-Tester-1.0.2-XSS-Access-Control.html\">View</a></
dd>\n</dl><p></p><h1>WordPress Contact Form Check Tester 1.0.2 XSS / Access Control</h1>\n<div>\n\n<pre><code>#
Exploit Title: WordPress Plugin Contact Form Check Tester 1.0.2 - Broken Access Control<br># Date: 2/28/2021<br>#
Author: 0xB9<br># Software Link: https://wordpress.org/plugins/contact-fo...ck-tester/<br># Version: 1.0.2<br>#
Tested on: Windows 10<br># CVE: CVE-2021-24247<br><br>1. Description:<br>The plugin settings are visible to all
registered users in the dashboard.<br>A registered user can leave a payload in the plugin settings.<br><br>2. Proof
of Concept:<br>- Register an account<br>- Navigate to the dashboard<br>- Go to CF7 Check Tester -&amp;gt; Settings<br>-
Add a form<br>- Add a field to the form<br>- Put in a payload in either Field selector or Field value
\"&amp;gt;&amp;lt;script&amp;gt;alert(1)&amp;lt;/script&amp;gt;<br>- Save<br>Anyone who visits the settings page will execute the
payload.<br><br></code></pre>\n</div>\n \n    \n    \n     </div>\n    \n      </div></div></body></html>",
    "id": "4/bnDLbGIuwgfYUHoNIoHFzwzucR/Wg3zKOf7t/Xc0Q=_17ebbb07b0d:f47321:aa31659c",
    "language": "en",
    "leoSummary": {
        "sentences": []
    },
    "origin": {
        "htmlUrl": "https://packetstormsecurity.com/",
        "streamId": "feed/http://packetstormsecurity.org/exploits.xml",
        "title": "Exploit Files \u2248 Packet Storm"
    },
    "originId": "https://packetstormsecurity.com/files/165814/wpcfct102-xssaccess.txt",
    "published": 1643820549000,
    "sources": [
        {
            "feedlyFeedType": "WebAlert",
            "searchTerms": {
                "isComplexFilter": false,
```

```
                "parts": [
                    {
                        "id": "nlp/f/publicationBucket/byf:cybersecurity-bundle",
                        "label": "Cybersecurity"
                    },
                    {
                        "text": "HIGH"
                    },
                    {
                        "id": "nlp/f/entity/wd:13166",
                        "label": "WordPress"
                    }
                ]
            },
            "streamId": "feed/https://feedly.com/f/alert/704a6215-d181-427e-b1a4-d50032e51968",
            "title": "Wordpress Vulns"
        }
    ],
    "summary": {
        "content": "WordPress Contact Form Check Tester plugin version 1.0.2 suffers from broken access control and
cross site scripting vulnerabilities.",
        "direction": "ltr"
    },
    "title": "WordPress Contact Form Check Tester 1.0.2 XSS / Access Control",
    "unread": true,
    "visual": {
        "url": "none"
    }
   }
  ],
  "updated": 1643836615133
}
```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
data.title	Object value	Report	WordPress Contact Form Check Tester 1.0.2 XSS / Access Control	N/A
data.published	object published_at	Published At	2022-02-17 17:11:52-00:00	Applied to all ingested objects
data.fullContent	Object description	Report		if `fullContent` does not exist, use `content`, if that doesn't exist, use `summary`
data.keywords	Attribute/ Tag	Tag	'Vulnerability Risk Management'	User chooses whether keywords is ingested as a tag or an attribute
data.consumergoods	Attribute	Affected Software	Windows 11	N/A
data.canonicalUrl	Attribute	Source URL	https://packetstormsecurity.com/files/165814/wpcfct102-xssaccess.txt	N/A
data.summary.content	Attribute	Feedly Summary	WordPress Contact Form Check Tester plugin version 1.0.2 suffers from broken access control and cross site scripting vulnerabilities.	Chosen first over data.leoSummary
data.leoSummary	Attribute	Feedly Leo Summary	"Over one million WordPress websites might have been impacted by a critical vulnerability in the Essential Addons for Elementor plugin."	Only used if data.summary doesn't exist
data.categories	Attribute	Feedly Category	Threat Intel	This attribute is the label of the feed it is associated with
data.estimatedCVSS.category	Attribute	Estimated CVSS Severity	High	Estimated CVSS severity that Feedly has provided
data.commonTopics	Attribute	Topic	Cyber Security	Topics that Feedly categorized the item under
data.cves	Object	CVE Indicator	CVE-2022-0190	User chooses whether CVE's are ingested as Indicators, Vulnerabilites or both
data.vulns	Object	Vulnerability	CVE-2022-0190	User chooses whether CVE's are ingested as Indicators, Vulnerabilites or both

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
data.fqdns	Object	FQDN Indicator	bzone.no-ip.biz	N/A
data.urls	Object	URL Indicator	https://sk5621.com.co	N/A
data.emailaddresses	Object	Email Address Indicator	N/A	N/A
data.ips	Object	IP Address Indicator	45.77.71.50:8082	N/A
data.md5	Object	MD5 Indicator	40b428899db353bb0ea244d95b5b82d9	N/A
data.sha1	Object	SHA-1 Indicator		N/A
data.sha256	Object	SHA-256 Indicator	6fcd36052b242bc33e90577e9a9cf5dc91bc7c5f3ad587b0d45ab4a7cb7b73b3	N/A
data.sha512	Object	SHA-512 Indicator	40b428899db353bb0ea244d95b5b82d9	N/A
data.mitreattacks	Object	Attack Pattern	T1187 - Forced Authentication	N/A
data.orgs	Object	Identity	Microsoft	N/A
data.malwarefamilies	Object	Malware	TrickBot	Includes attribute of affected OS
data.threatactors	Object	Adversary	MuddyWater	N/A

Average Feed Run

The following results were obtained with both **Indicators** and **Vulnerabilities** selected as the type of CVE to ingest and both **Tags** and **Attributes** selected as the type for keywords to ingest. There may be more or less objects depending on feed.

METRIC	RESULT
Run Time	< 1 minute
Adversary	1
Attack Pattern	27
Identity	5
Indicators	85
Indicator Attributes	20
Malware	3
Report	13
Report Attributes	69
Vulnerability	6

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.

Known Issues / Limitations

- You cannot pull from a Personal Feed. You can only pull from streams/feeds that are listed under your Team Feeds.
- When CVE's are ingested as Vulnerabilities, `published_at` and attributes are not applied due to a shallow copy bug.

Change Log

- **Version 1.0.0**
  - Initial release