ThreatQuotient

Flashpoint VulnDB CDF

Version 1.0.0

May 06, 2024

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	1.0.0
Compatible with ThreatQ Versions	>= 5.19.0
Support Tier	ThreatQ Supported

Introduction

The Flashpoint VulnDB CDF integration leverages VulnDB to provide ThreatQ users with the latest information on vulnerabilities, including details on affected software, severity, and remediation steps.

Flashpoint's VulnDB is a vulnerability database designed to help organizations manage risk. It boasts a comprehensive collection of up-to-date vulnerabilities, including those not listed elsewhere, and offers alerts to keep users informed. By providing information on both end-user software and third-party libraries, VulnDB helps organizations address security weaknesses across their entire IT infrastructure.

By integrating VulnDB with ThreatQ, users can quickly identify and address vulnerabilities that pose a risk to their organization.

The integration provides the following feed:

- **Flashpoint VulnDB** - ingests vulnerabilities & related CVEs from VulnDB.

The integration ingests indicator and Vulnerability object types.

Prerequisites

The following is required for the integration:

- A Flashpoint VulnDB License.

  This license is separate from the Ignite and FP Tools.

- Flashpoint API Credentials.

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 yaml file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration yaml file using one of the following methods:
   - Drag and drop the file into the dialog box
   - Select **Click to Browse** to locate the 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. The feed will be added to the integrations page. 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 integration-related credentials.

To configure the integration:

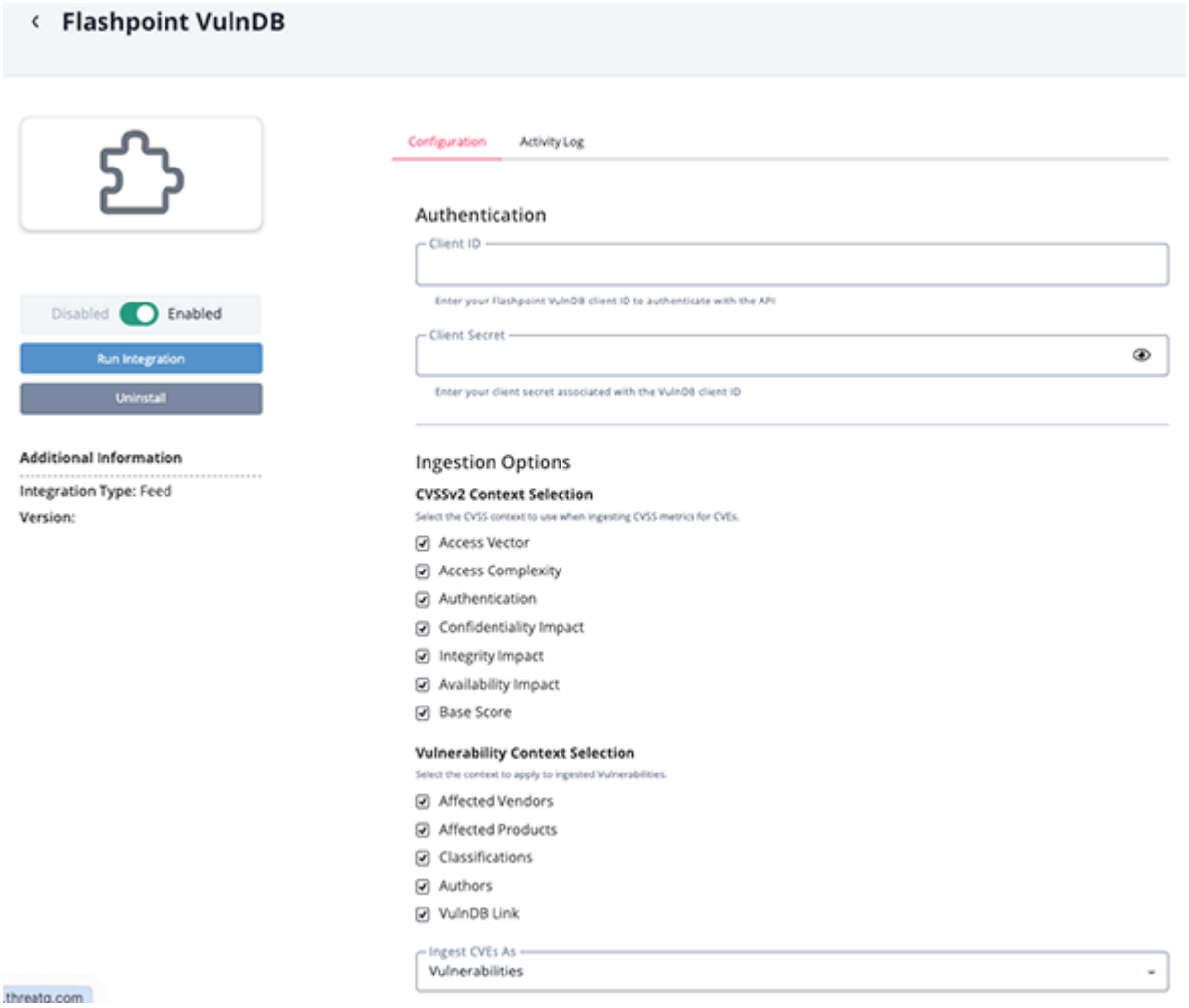
1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** option from the *Category* dropdown (optional).

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

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

PARAMETER	DESCRIPTION
Client ID	Enter your Flashpoint VulnDB client ID to authenticate with the API.
Client Secret	Enter your client secret associated with the VulnDB client ID.
CVSSv2 Context Selection	Select the CVSS context to use when ingesting CVSS metrics for CVEs. Options include: ◦ Access Vector ◦ Access Complexity ◦ Authentication ◦ Confidentiality Impact ◦ Integrity Impact ◦ Availability Impact ◦ Base Score *(default)*
Vulnerability Context Selection	Select the context to apply to ingested Vulnerabilities. Options include: ◦ Affected Vendors *(default)* ◦ Affected Products *(default)* ◦ Classification *(default)* ◦ Authors ◦ VulnDB Link

PARAMETER	DESCRIPTION
Ingest CVEs as	Select the entity type to ingest CVEs as. Options include: ◦ Indicators ◦ Vulnerabilities *(default)*



5. Review any additional settings, 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

Flashpoint VulnDB

The Flashpoint VulnDB feed pulls vulnerabilities & CVEs from Flashpoint's VulnDB. This feed is designed to provide the latest information on vulnerabilities, including details on affected software, severity, and remediation steps.

`GET https://vulndb.flashpoint.io/api/v1/vulnerabilities/find_by_date`

Sample Response:


```
{
  "total_entries": 1,
  "current_page": 1,
  "results": [
    {
      "vulndb_id": 3726,
      "title": "BEA WebLogic HTTP TRACE Response XSS",
      "keywords": " ",
      "description": "WebLogic Server and Express contain a flaw that allows a
remote cross site scripting attack. This flaw exists because the application
does not validate HTTP TRACE requests upon submission to the server. This could
allow a user to create a specially crafted URL that would execute arbitrary
code in a user's browser within the trust relationship between the browser and
the server, leading to a loss of integrity.",
      "solution": "Currently, there are no known workarounds or upgrades to
correct this issue. \nHowever, Bea has released a patch to address this
vulnerability.",
      "vulndb_published_date": "",
      "vulndb_last_modified": "2024-04-01T15:30:33Z",
      "manual_notes": "",
      "t_description": "",
      "solution_date": "",
      "disclosure_date": "2004-01-27T09:17:35Z",
      "discovery_date": "",
      "exploit_publish_date": "",
      "vendor_informed_date": "",
      "vendor_ack_date": "",
      "third_party_solution_date": "",
      "ext_references": [
        {
          "value": "http://dev2dev.bea.com/resourcelibrary/
advisoriesnotifications/BEA04_48.00.jsp",
          "type": "Vendor Specific Advisory URL"
        },
        {
          "value": "14959",
```

```
          "type": "ISS X-Force ID"
        },
        {
          "value": "9506",
          "type": "Bugtraq ID"
        },
        {
          "value": "2004-2320",
          "type": "CVE ID"
        },
        {
          "value": "http://dev2dev.bea.com/pub/advisory/68",
          "type": "Other Advisory URL"
        },
        {
          "value": "493",
          "type": "SCIP VulDB ID"
        },
        {
          "value": "https://support.f5.com/kb/en-us/solutions/public/15000/900/
sol15904.html",
          "type": "Vendor Specific Advisory URL"
        },
        {
          "value": "http://www.collax.com/fileadmin/collax_upload/downloads/
downloads_c_server/CBS/Release_Notes_EN/relnotes-cbs-7.0.20.en.html",
          "type": "Vendor Specific Advisory URL"
        }
      ],
      "cvss_metrics": [
        {
          "id": 81524,
          "access_vector": "NETWORK",
          "access_complexity": "MEDIUM",
          "authentication": "NONE",
          "confidentiality_impact": "PARTIAL",
          "integrity_impact": "PARTIAL",
          "availability_impact": "NONE",
          "source": "http://nvd.nist.gov",
          "generated_on": "2005-08-18T08:38:00Z",
          "cve_id": "2004-2320",
          "score": 5.8,
          "calculated_cvss_base_score": 5.8
        }
      ],
      "vendors": [
        {
          "vendor": {
            "id": 1204,
            "name": "BEA Systems, Inc."
```

```
          }
        },
        {
          "vendor": {
            "id": 1222,
            "name": "Oracle Corporation"
          }
        }
      ],
      "products": [
        {
          "id": 1936,
          "name": "BEA WebLogic Express",
          "versions": [
            {
              "id": 4338,
              "name": "5.1 Service Pack 13",
              "affected": "true"
            },
            {
              "id": 4339,
              "name": "6.1 SP6",
              "affected": "true"
            },
            {
              "id": 4340,
              "name": "7.0 SP4",
              "affected": "true"
            },
            {
              "id": 4341,
              "name": "8.1 SP2",
              "affected": "true"
            }
          ]
        }
      ],
      "classifications": [
        {
          "id": 2,
          "name": "location_remote",
          "longname": "Remote / Network Access",
          "description": "This vulnerability can be exploited over a wired
network (e.g., LAN, WAN, Internet)."
        },
        {
          "id": 12,
          "name": "attack_type_input_manip",
          "longname": "Input Manipulation",
          "description": "A vulnerability that is exploited by sending
```

```
manipulated and unexpected data to a service or process. This includes all
types of overflows, memory corruption, XSS, SQLi, RFI, traversals and more."
        },
        {
          "id": 18,
          "name": "impact_integrity",
          "longname": "Loss of Integrity",
          "description": "Assurance that data is unaltered by unauthorized
persons and authorization has not been exceeded.\r\nExamples: XSS, arbitrary
command execution, most overflows, most format strings, SQL injection,
unauthorized file modification/deletion/creation, remote file inclusion, etc."
        },
        {
          "id": 24,
          "name": "exploit_unknown",
          "longname": "Exploit Unknown",
          "description": "The status of a working exploit is unknown."
        },
        {
          "id": 29,
          "name": "vuln_web_check",
          "longname": "Web Related",
          "description": "A vulnerability in an HTTP(S) related product."
        }
      ],
      "authors": []
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.title`	Vulnerability Value	N/A	`.vulndb_published_date` or `.disclosure_date`	N/A	N/A
`.keywords`	Vulnerability Tag/ CVE Tags	N/A	N/A	`CWE-93`	Split by comma
`.products[]`	Vulnerability Attribute/ CVE Attribute	Affected Product	`.vulndb_published_date` or `.disclosure_date`	`NorthStar Controller Application`	Optional
`.vendors[].vendor.name`	Vulnerability Attribute/ CVE Attribute	Affected Vendor	`.vulndb_published_date` or `.disclosure_date`	`Canonical`	Optional
`.classifications[].longname`	Vulnerability Attribute/ CVE Attribute	Classification	`.vulndb_published_date` or `.disclosure_date`	`Remote / Network Access`	Optional
`.authors[].longname`	Vulnerability Attribute	Author	`.vulndb_published_date` or `.disclosure_date`	N/A	Optional
`.vulndb_id`	Vulnerability Attribute	VulnDB Link	`.vulndb_published_date` or `.disclosure_date`	N/A	Optional
`.cvss_metrics[].access_vector`	CVE Attribute	CVSSv2 Access Vector	N/A	`NETWORK`	Optional
`.cvss_metrics[].access_complexity`	CVE Attribute	CVSSv2 Access Complexity	N/A	`MEDIUM`	Optional
`.cvss_metrics[].authentication`	CVE Attribute	CVSSv2 Authentication	N/A	`NONE`	Optional
`.cvss_metrics[].confidentiality_impact`	CVE Attribute	CVSSv2 Confidentiality Impact	N/A	`PARTIAL`	Optional
`.cvss_metrics[].integrity_impact`	CVE Attribute	CVSSv2 Integrity Impact	N/A	`PARTIAL`	Optional
`.cvss_metrics[].availability_impact`	CVE Attribute	CVSSv2 Availability Impact	N/A	`NONE`	Optional
`.cvss_metrics[].score`	CVE Attribute	CVSSv2 Base Score	N/A	`5.8`	Optional
`.cvss_metrics[].cve_id`	Vulnerability Value, Indicator value	CVE	N/A	`CVE-2024-12345`	Ingested entity based on `Ingest CVEs As` user field
`.ext_references[].value`	Vulnerability Value, Indicator value	CVE	N/A	`CVE-2024-12345`	Ingested entity based on `Ingest CVEs As` user field; If `.type == CVE ID`

Average Feed Run

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.

METRIC	RESULT
Run Time	31 minutes
Vulnerabilities	3,685
Vulnerability Attributes	101,664

Change Log

- **Version 1.0.0**
  - Initial release