ThreatQuotient

A Securonix Company

Flashpoint Ignite Vulnerabilities CDF

Version 1.1.1

August 19, 2025

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	1.1.1
Compatible with ThreatQ Versions	>= 5.25.0
Support Tier	ThreatQ Supported

Introduction

The Flashpoint Ignite Vulnerabilities CDF ingests threat intelligence data from the Flashpoint Ignite API as either indicators or vulnerabilities based on user settings.

The integration provides the following feed:

- **Flashpoint Ignite Vulnerabilities** - ingests vulnerabilities and indicators from the Flashpoint Ignite API.

The integration ingests ether indicators or vulnerabilities system object based on user settings.

Prerequisites

The following is required to run the integration:

- A Flashpoint Ignite API Token.

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 yaml file into the dialog box
   - Select **Click to Browse** to locate the integration yaml 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.

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:

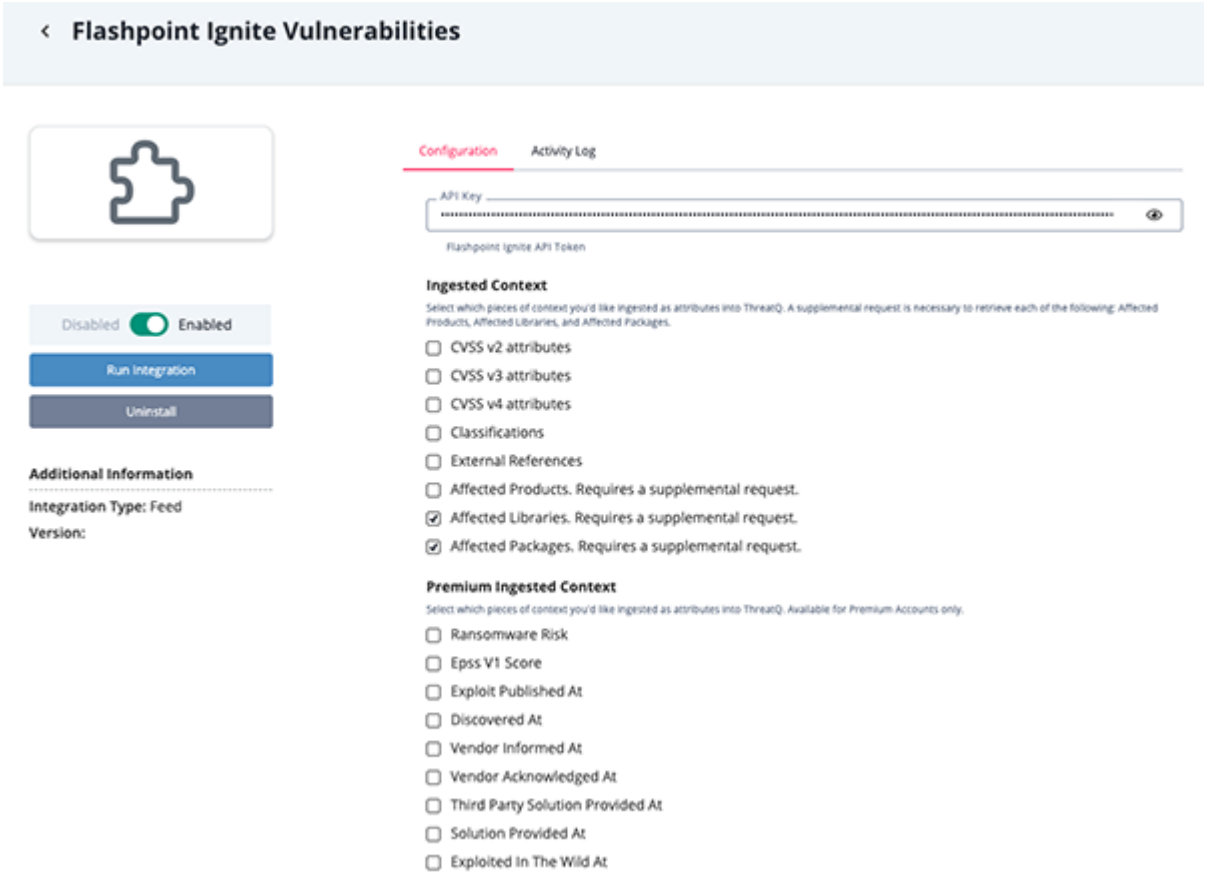
1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** option from the *Category* dropdown (optional).

   > 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
API Key	Enter your Flashpoint Ignite API token.
Ingested Context	Select the pieces of context to ingest as attributes into the ThreatQ platform. Options include: ◦ CVSS v2 attributes *(default)* ◦ CVSS v3 attributes *(default)* ◦ CVSS v4 attributes ◦ Classifications *(default)* ◦ External References *(default)* ◦ Affected Products *(default)* ◦ Affected Libraries ◦ Affected Packages
Premium Ingested Context	Select the pieces of premium context to ingest as attributes into the ThreatQ platform. > This option is only available for FlashPoint Premium accounts. Options include:

PARAMETER	DESCRIPTION
	◦ Ransomware Risk (default) ◦ Epss V1 Score (default) ◦ Exploit Published At (default) ◦ Discovered At (default) ◦ Vendor Informed At ◦ Vendor Acknowledged At ◦ Third Party Solution Provided At ◦ Solution Provided At ◦ Exploited In The Wild At
Save CVE Data As	Select how to ingest the threat data into the platform. Options include: ◦ Vulnerabilities (default) ◦ Indicators
Disable Proxies	Enable this option to have the feed ignore proxies set in the ThreatQ UI.
Enable SSL Verification	Enable this option if the feed should verify the SSL certificate.



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 Ignite Vulnerabilities

The Flashpoint Ignite Vulnerabilities feeds ingests threat intelligence data from the Flashpoint Ignite API. This data is saved in the form of vulnerabilities or indicators based on the feed configurations.

`GET api.flashpoint.io/vulnerability-intelligence/v1/vulnerabilities`

Sample Response:


```
{
  "total": 246673,
  "next": "https://api.flashpoint.io/api/v1/vulnerabilities/?from=20size=20",
  "previous": null,
  "size": 20,
  "from": 0,
  "results": [
    {
      "id": 351481,
      "title": "pdfmake dev-playground/server.js createPdfBinary() Function /
pdf Endpoint content Parameter Handling Remote Code Execution",
      "keywords": "",
      "description": "pdfmake contains a flaw in the createPdfBinary() function
in dev-playground/server.js that is triggered as user-supplied input in the
'content' parameter is used with the Function class. With a specially crafted
POST request to the /pdf endpoint, a remote attacker can execute arbitrary
code.",
      "solution": "We are not currently aware of a solution for this
vulnerability.",
      "timelines": {
        "disclosed_at": "2024-02-27T00:00:00Z",
        "published_at": "2024-03-05T08:35:30Z",
        "last_modified_at": "2024-03-05T08:35:30Z"
      },
      "scores": {
        "epss_score": 0.00043,
        "severity": "Critical"
      },
      "vuln_status": "Active",
      "cwes": [],
      "ext_references": [
        {
          "value": "2024-25180",
          "type": "CVE ID",
          "created_at": "2024-02-29T19:33:53Z"
        },
        {
```

```
          "value": "https://github.com/joaoviictorti/My-CVES/blob/main/
CVE-2024-25180/README.md",
          "type": "Other Advisory URL",
          "created_at": "2024-02-29T19:33:53Z"
        }
      ],
      "classifications": [
        {
          "name": "location_remote",
          "longname": "Remote / Network Access",
          "description": "This vulnerability can be exploited over a wired
network (e.g., LAN, WAN, Internet)."
        }
      ],
      "cvss_v2s": [
        {
          "access_vector": "NETWORK",
          "access_complexity": "LOW",
          "authentication": "NONE",
          "confidentiality_impact": "COMPLETE",
          "integrity_impact": "COMPLETE",
          "availability_impact": "COMPLETE",
          "source": "Flashpoint",
          "generated_on": "2024-03-05T08:30:56Z",
          "cve_id": null,
          "score": 10,
          "calculated_cvss_base_score": null
        }
      ],
      "cvss_v3s": [
        {
          "attack_vector": "NETWORK",
          "attack_complexity": "LOW",
          "privileges_required": "NONE",
          "user_interaction": "NONE",
          "scope": "UNCHANGED",
          "confidentiality_impact": "HIGH",
          "integrity_impact": "HIGH",
          "availability_impact": "HIGH",
          "source": "Flashpoint",
          "generated_on": "2024-03-05T08:30:56Z",
          "cve_id": null,
          "score": 9.8,
          "calculated_cvss_base_score": null,
          "vector_string": "CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/
RL:U/RC:U",
          "version": "3.1"
        }
      ],
      "nvd_additional_information": [],
```

```
      "products": [
        {
          "id": 13058826,
          "name": "pdfmake"
        }
      ],
      "vendors": [
        {
          "id": 12436653,
          "name": "Bartek Pampuch"
        }
      ]
    }
]
}
```

Default Mapping Table

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
CVE-(.results[].ext_references[].value)	Indicator.Value/ Vulnerability.Value	CVE (for Indicators)	.results[].timelines.published_at	CVE-2024-25180	If `.results[].ext_references[].type` is "CVE ID"
.results[].description	indicator.description/ vulnerability.description	N/A	.results[].timelines.published_at	pdfmake contains a flaw in the createPdfBinary() function in dev-playground/ server.js...	
.results[].solution	Indicator.Attribute/ Vulnerability.Attribute	Summary	.results[].timelines.published_at	We are not currently aware of a solution for this vulnerability.	
.results[].scores.severity	Indicator.Attribute/ Vulnerability.Attribute	Severity	.results[].timelines.published_at	Critical	Updatable.
.results[].scores.epss_score	Indicator.Attribute/ Vulnerability.Attribute	EPSS Score	.results[].timelines.published_at	0.00043	Updatable.
.results[].cvss_v2s[].access_complexity	Indicator.Attribute/ Vulnerability.Attribute	CVSSV2 Access Complexity	.results[].timelines.published_at	LOW	User-configurable.Updatable.
.results[].cvss_v2s[].access_vector	Indicator.Attribute/ Vulnerability.Attribute	CVSSV2 Access Vector	.results[].timelines.published_at	NETWORK	User-configurable.Updatable.
.results[].cvss_v2s[].authentication	Indicator.Attribute/ Vulnerability.Attribute	CVSSV2 Authentication	.results[].timelines.published_at	NONE	User-configurable.
.results[].cvss_v2s[].availability_impact	Indicator.Attribute/ Vulnerability.Attribute	CVSSV2 Availability Impact	.results[].timelines.published_at	COMPLETE	User-configurable.Updatable.
.results[].cvss_v2s[].score	Indicator.Attribute/ Vulnerability.Attribute	CVSSV2 Score	.results[].timelines.published_at	10	User-configurable.Updatable.
.results[].cvss_v2s[].confidentiality_impact	Indicator.Attribute/ Vulnerability.Attribute	CVSSV2 Confidentiality Impact	.results[].timelines.published_at	COMPLETE	User-configurable.Updatable.
.results[].cvss_v2s[].calculated_cvss_base_score	Indicator.Attribute/ Vulnerability.Attribute	CVSSV2 Calculated CVSS Base Score	.results[].timelines.published_at	10	User-configurable.Updatable.
.results[].cvss_v2s[].integrity_impact	Indicator.Attribute/ Vulnerability.Attribute	CVSSV2 Integrity Impact	.results[].timelines.published_at	COMPLETE	User-configurable.Updatable.
.results[].cvss_v3s[].attack_complexity	Indicator Attribute/ Vulnerability.Attribute	CVSSV3 Attack Complexity	.results[].timelines.published_at	LOW	User-configurable.Updatable.
.results[].cvss_v3s[].attack_vector	Indicator.Attribute/ Vulnerability.Attribute	CVSSV3 Attack Vector	.results[].timelines.published_at	NETWORK	User-configurable.Updatable.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.results[].cvss_v3s[].privileges_required	Indicator.Attribute/ Vulnerability.Attribute	CVSSV3 Privileges Required	.results[].timelines.published_at	NONE	User-configurable.
.results[].cvss_v3s[].availability_impact	Indicator.Attribute/ Vulnerability.Attribute	CVSSV3 Availability Impact	.results[].timelines.published_at	HIGH	User-configurable.Updatable.
.results[].cvss_v3s[].score	Indicator.Attribute/ Vulnerability.Attribute	CVSSV3 Score	.results[].timelines.published_at	9.8	User-configurable.Updatable.
.results[].cvss_v3s[].confidentiality_impact	Indicator.Attribute/ Vulnerability.Attribute	CVSSV3 Confidentiality Impact	.results[].timelines.published_at	HIGH	User-configurable.Updatable.
.results[].cvss_v3s[].calculated_cvss_base_score	Indicator.Attribute/ Vulnerability.Attribute	CVSSV3 Calculated CVSS Base Score	.results[].timelines.published_at	9.8	User-configurable.Updatable.
.results[].cvss_v3s[].integrity_impact	Indicator.Attribute/ Vulnerability.Attribute	CVSSV3 Integrity Impact	.results[].timelines.published_at	HIGH	User-configurable.Updatable.
.results[].cvss_v3s[].scope	Indicator.Attribute/ Vulnerability.Attribute	CVSSV3 Scope	.results[].timelines.published_at	UNCHANGED	User-configurable.Updatable.
.results[].cvss_v3s[].vector_string	Indicator.Attribute/ Vulnerability.Attribute	CVSSV3 Vector String	.results[].timelines.published_at	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:U/RC:U	User-configurable.
.results[].cvss_v3s[].user_interaction	Indicator.Attribute/ Vulnerability.Attribute	CVSSV3 User Interaction	.results[].timelines.published_at	NONE	User-configurable.
.results[].products[].name	Indicator.Attribute/ Vulnerability.Attribute	Product Name	.results[].timelines.published_at	pdfmake	
.results[].vendors[].name	Indicator.Attribute/ Vulnerability.Attribute	Product Vendor	.results[].timelines.published_at	Bartek Pampuch	
.results[].classifications[].description	Indicator.Attribute/ Vulnerability.Attribute	"Classification - "+.results[].classifications[].longname	.results[].timelines.published_at	This vulnerability can be exploited over a wired network (e.g., LAN, WAN, Internet).	User-configurable.
.results[].timelines.last_modified_at	Indicator.Attribute/ Vulnerability.Attribute	Last Modified At	.results[].timelines.published_at	2024-03-05T08:45:32Z	Timestamp. Updatable.
.results[].ext_references[].value	Indicator.Attribute/ Vulnerability.Attribute	.results[].ext_references[].type(Other Advisory URL)	.results[].timelines.published_at	https://github.com/joaoviictorti/My-CVES/blob/main/CVE-2024-25180/README.md	User-configurable.

Premium Flashpoint Accounts Mapping Table

ThreatQuotient provides the following default mapping for Premium Flashpoint accounts:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.results[].cvss_v3s[].updated_at	Indicator Attribute/ Vulnerability.Attribute	CVSSV3 Updated At	.results[].timelines. published_at	N/A	Timestamp. User-configurable. Updatable.
.results[].cvss_v3s[].temporal_ score	Indicator.Attribute/ Vulnerability.Attribute	CVSSV3 Temporal Score	.results[].timelines. published_at	N/A	User-configurable. Updatable.
.results[].cvss_v3s[].remediation_ level	Indicator.Attribute/ Vulnerability.Attribute	CVSSV3 Remediation Level	.results[].timelines. published_at	N/A	User-configurable. Updatable.
.results[].cvss_v3s[].exploit_code_ maturity	Indicator.Attribute/ Vulnerability.Attribute	CVSSV3 Exploit Maturity	.results[].timelines. published_at	N/A	User-configurable. Updatable.
.results[].cvss_v3s[].report_ confidence	Indicator.Attribute/ Vulnerability.Attribute	CVSSV3 Report confidence	.results[].timelines. published_at	N/A	User-configurable. Updatable.
.results[].cvss_v4s[].attack_ complexity	Indicator.Attribute/ Vulnerability.Attribute	CVSSV4 Attack Complexity	.results[].timelines. published_at	N/A	User-configurable. Updatable.
.results[].cvss_v4s[].attack_ vector	Indicator.Attribute/ Vulnerability.Attribute	CVSSV4 Attack Vector	.results[].timelines. published_at	N/A	User-configurable.
.results[].cvss_v4s[]. privileges_required	Indicator.Attribute/ Vulnerability.Attribute	CVSSV4 Privileges Required	.results[].timelines. published_at	N/A	User-configurable.
.results[].cvss_v4s[].score	Indicator.Attribute/ Vulnerability.Attribute	CVSSV4 Score	.results[].timelines. published_at	N/A	User-configurable. Updatable.
.results[].cvss_v4s[].vector_ string	Indicator.Attribute/ Vulnerability.Attribute	CVSSV4 Vector String	.results[].timelines. published_at	N/A	User-configurable.
.results[].cvss_v4s[].user_ interaction	Indicator.Attribute/ Vulnerability.Attribute	CVSSV4 User Interaction	.results[].timelines. published_at	N/A	User-configurable. Updatable.
.results[].cvss_v4s[].exploit_ code_maturity	Indicator.Attribute/ Vulnerability.Attribute	CVSSV4 Exploit Maturity	.results[].timelines. published_at	N/A	User-configurable. Updatable.
.results[].cvss_v4s[].threat_ score	Indicator.Attribute/ Vulnerability.Attribute	CVSSV4 Threat Score	.results[].timelines. published_at	N/A	User-configurable. Updatable.
.results[].cvss_v4s[].vulnerable_ system_confidentiality_impact	Indicator.Attribute/ Vulnerability.Attribute	CVSSV4 Vulnerable System Confidentiality Impact	.results[].timelines. published_at	N/A	User-configurable. Updatable.
.results[].cvss_v4s[].vulnerable_ system_integrity_impact	Indicator.Attribute/ Vulnerability.Attribute	CVSSV4 Vulnerable System Integrity Impact	.results[].timelines. published_at	N/A	User-configurable. Updatable.
.results[].cvss_v4s[].vulnerable_ system_availability_impact	Indicator.Attribute/ Vulnerability.Attribute	CVSSV4 Vulnerable System Availability Impact	.results[].timelines. published_at	N/A	User-configurable. Updatable.
.results[].scores.ransomware_ score	Indicator.Attribute/ Vulnerability.Attribute	Ransomware Risk	.results[].timelines. published_at	N/A	User-configurable.Updatable.
.results[].scores.epss_v1_ score	Indicator.Attribute/ Vulnerability.Attribute	EPSS V1 Score	.results[].timelines. published_at	N/A	User-configurable.Updatable.
.results[].timelines.exploit_ published_at	Indicator.Attribute/ Vulnerability.Attribute	Exploit Published At	.results[].timelines. published_at	N/A	Timestamp. User-configurable. Updatable.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.results[].timelines.discovered_at	Indicator.Attribute/ Vulnerability.Attribute	Discovered At	.results[].timelines.published_at	N/A	Timestamp. User-configurable. Updatable.
.results[].timelines.vendor_informed_at	Indicator.Attribute/ Vulnerability.Attribute	Vendor Informed At	.results[].timelines.published_at	N/A	Timestamp. User-configurable. Updatable.
.results[].timelines.vendor_acknowledged_at	Indicator.Attribute/ Vulnerability.Attribute	Vendor Acknowledged At	.results[].timelines.published_at	N/A	Timestamp. User-configurable. Updatable.
.results[].timelines.third_party_solution_provided_at	Indicator.Attribute/ Vulnerability.Attribute	Third Party Solution Provided At	.results[].timelines.published_at	N/A	Timestamp. User-configurable. Updatable.
.results[].timelines.solution_provided_at	Indicator.Attribute/ Vulnerability.Attribute	Solution Provided At	.results[].timelines.published_at	N/A	Timestamp. User-configurable. Updatable.
.results[].timelines.exploited_in_the_wild_at	Indicator.Attribute/ Vulnerability.Attribute	Exploited In The Wild At	.results[].timelines.published_at	N/A	Timestamp. User-configurable. Updatable.

Get Vulnerability Affected Products (Supplemental)

The Get Vulnerability Affected Products supplemental feed uses the vulnerability `results[].id` to request vulnerability details and ingest product information.

`GET api.flashpoint.io/vulnerability-intelligence/v1/vulnerabilities/{id}`

Sample Response:


```
{
  "id": 389836,
  "cve_ids": [
    "CVE-2025-23007"
  ],
  "title": "SonicWall NetExtender for Windows Log Export Functionality Improper
Privilege Management Local Privilege Escalation",
  "keywords": "",
  "description": "SonicWall NetExtender contains a flaw in the Log Export
functionality that is triggered as privileges are not properly managed. This
may allow a local attacker to disclose system files, potentially resulting in
privilege escalation.",
  "solution": "It has been reported that this has been fixed. Please refer to
the product listing for upgraded versions that address this vulnerability.",
  "technical_description": "While exploitation of this issue has an immediate
follow-up impact of allowing an attacker to escalate privileges, please note
the discrepancy in the CVSSv2 and CVSSv3 scores. The immediate impact is
disclosure of system files and has been scored as such for CVSSv2 in accordance
with the CVSSv2 guidelines. These specify that follow-up impacts should not be
considered. A scoring policy change means that follow-up impacts should be
considered for CVSSv3. This is one of the few changes to CVSS, where CVSSv3
produces more reliable scores than CVSSv2.\r\n\r\nPlease note that this
vulnerability only affects versions for Windows.",
  "timelines": {
    "published_at": "2025-01-30T22:52:06Z",
    "last_modified_at": "2025-02-03T22:55:13Z",
    "exploit_published_at": "2025-01-30T00:00:00Z",
    "discovered_at": null,
    "disclosed_at": "2025-01-30T00:00:00Z",
    "vendor_informed_at": null,
    "vendor_acknowledged_at": null,
    "third_party_solution_provided_at": null,
    "solution_provided_at": "2025-01-30T00:00:00Z",
    "exploited_in_the_wild_at": null,
    "vendor_response_time": null,
    "time_to_patch": null,
    "total_time_to_patch": null,
    "time_unpatched": "0:00:00",
    "time_to_exploit": "0:00:00",
    "total_time_to_exploit": null
  },
  "scores": {
```

```
    "epss_score": 0.00043,
    "epss_v1_score": 0.0033334729,
    "ransomware_score": "Low",
    "severity": "High",
    "social_risk_scores": [
      {
        "cve_id": "CVE-2025-23007",
        "numeric_score": 0.4348443,
        "categorical_score": "LOW",
        "score_date": "2025-02-06T00:00:00Z",
        "todays_tweets": 0,
        "total_tweets": 6,
        "unique_users": 6
      }
    ]
  },
  "vuln_status": "Active",
  "alternate_vulndb_id": null,
  "changelog": [
    {
      "created_at": "2025-01-30T22:52:06Z",
      "description": "Vulnerability Added: SonicWall NetExtender for Windows
Log Export Functionality Improper Privilege Management Local Privilege
Escalation Created"
    }
  ],
  "cwes": [
    {
      "cwe_id": 269,
      "name": "Improper Privilege Management",
      "source": "flashpoint",
      "cve_ids": "2025-23007"
    }
  ],
  "exploits": [],
  "exploits_count": 0,
  "ext_references": [
    {
      "value": "https://psirt.global.sonicwall.com/vuln-detail/
SNWLID-2025-0005",
      "type": "Vendor Specific Advisory URL",
      "created_at": "2025-01-30T09:45:33Z"
    }
  ],
  "nvd_additional_information": [
    {
      "cve_id": "CVE-2025-23007",
      "summary": "A vulnerability in the NetExtender Windows client log export
function allows unauthorized access to sensitive Windows system files,
potentially leading to privilege escalation.",
```

```
      "cwes": [
        {
          "cwe_id": 276,
          "name": "Incorrect Default Permissions"
        }
      ],
      "references": [
        {
          "name": "https://psirt.global.sonicwall.com/vuln-detail/
SNWLID-2025-0005",
          "url": "https://psirt.global.sonicwall.com/vuln-detail/
SNWLID-2025-0005"
        }
      ],
      "cvss_v2s": [],
      "cvss_v3s": []
    }
  ],
  "classifications": [
    {
      "name": "location_local",
      "longname": "Local Access Required",
      "description": "Local access is required to exploit this vulnerability
(e.g., unix shell, windows user)."
    }
  ],
  "creditees": [
    {
      "name": "Eduardo Pérez-Malumbres Cervera"
    }
  ],
  "cvss_v2s": [
    {
      "access_vector": "LOCAL",
      "access_complexity": "LOW",
      "authentication": "NONE",
      "confidentiality_impact": "PARTIAL",
      "integrity_impact": "NONE",
      "availability_impact": "NONE",
      "source": "Flashpoint",
      "generated_at": "2025-01-30T17:11:06Z",
      "cve_id": null,
      "score": 2.1,
      "calculated_cvss_base_score": 2.1
    }
  ],
  "cvss_v3s": [
    {
      "attack_vector": "LOCAL",
      "attack_complexity": "LOW",
```

```
      "privileges_required": "LOW",
      "user_interaction": "NONE",
      "scope": "CHANGED",
      "confidentiality_impact": "HIGH",
      "integrity_impact": "HIGH",
      "availability_impact": "HIGH",
      "source": "Flashpoint",
      "generated_at": "2025-01-30T22:50:00Z",
      "cve_id": null,
      "score": 8.8,
      "calculated_cvss_base_score": 8.8,
      "vector_string": "CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:F/RL:O/
RC:C",
      "version": "3.1",
      "remediation_level": "OFFICIAL_FIX",
      "report_confidence": "CONFIRMED",
      "exploit_code_maturity": "FUNCTIONAL",
      "temporal_score": 8.2,
      "updated_at": "2025-01-30T22:52:06Z"
    }
  ],
  "cvss_v4s": [
    {
      "score": 9.3,
      "threat_score": 9.3,
      "source": "Flashpoint",
      "generated_at": "2025-01-30T22:51:09.024000Z",
      "updated_at": "2025-01-30T22:51:09.051000Z",
      "cve_id": null,
      "vector_string": "CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/
SI:H/SA:H/E:A",
      "version": "4.0",
      "attack_vector": "LOCAL",
      "attack_complexity": "LOW",
      "attack_requirements": "NONE",
      "privileges_required": "LOW",
      "user_interaction": "NONE",
      "exploit_maturity": "ATTACKED",
      "vulnerable_system_confidentiality_impact": "HIGH",
      "vulnerable_system_integrity_impact": "HIGH",
      "vulnerable_system_availability_impact": "HIGH",
      "subsequent_system_confidentiality_impact": "HIGH",
      "subsequent_system_integrity_impact": "HIGH",
      "subsequent_system_availability_impact": "HIGH"
    }
  ],
  "tags": [
    "pre_nvd"
  ],
  "products": [
```

```
    {
      "id": 1828632,
      "name": "SonicWall NetExtender",
      "versions": [
        {
          "id": 1945178,
          "vulndb_version_id": 6248,
          "name": "10.3.0",
          "affected": "Affected",
          "all_prior_versions_affected": true,
          "cpes": []
        }
      ],
      "vendor_id": 1756,
      "vendor": "Dell"
    }
  ]
}
```


ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.products.name, .versions[].name, .versions[].affected	Indicator.Attribute/ Vulnerability.Attribute	Affected Product	.results[].timelines.published_at	SonicWall NetExtender, version 10.3.0 - Affected	User-configurable. Value composed from different attributes for Premium policies only
.products.name	Indicator.Attribute/ Vulnerability.Attribute	Affected Product	.results[].timelines.published_at	SonicWall NetExtender	User-configurable. For non-Premium policies

Get Vulnerability Affected Libraries (Supplemental)

The Get Vulnerability Affected Libraries supplemental feed uses the vulnerability `results[].id` to request vulnerability Libraries if the product is affected, information received if Affected Products is checked for premium accounts, and the user selected the option in Ingested Context.

`GET api.flashpoint.io/vulnerability-intelligence/v1/vulnerabilities/{id}/libraries`

Sample Response:

```
{
  "total": 1,
  "next": null,
  "previous": null,
  "size": 25,
  "from": 0,
  "results": [
    {
      "id": 113566,
      "namespace": "-",
      "name": "libtiff",
      "version": "4.7.0",
      "qualifiers": "-",
      "subpath": "-",
      "type": "conan",
      "purl": "pkg:conan"
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.results[].name, .results[].version	Indicator.Attribute/ Vulnerability.Attribute	Affected Library	.results[].timelines. published_at	libtiff, version 4.7.0	User-configurable. Value composed from different attributes. Only ingested if the Product is affected and `Affected Products` is checked.

Get Vulnerability Affected Packages (Supplemental)

The Get Vulnerability Affected Packages supplemental feed uses the vulnerability results[].id to request vulnerability Packages, if the product is affected, information received if Affected Products is checked for premium accounts, and the user selected the option in Ingested Context.

`GET api.flashpoint.io/vulnerability-intelligence/v1/vulnerabilities/{id}/packages`

Sample Response:


```
{
  "total": 53,
  "next": "https://api.flashpoint.io/vulnerability-intelligence/v1/
vulnerabilities/412754/packages?from=25size=25",
  "previous": null,
  "size": 25,
  "from": 0,
  "results": [
    {
      "id": 2755425,
      "name": "ruby-thor",
      "version": "1.0.1-1",
      "filename": "ruby-thor_1.0.1-1_all.deb",
      "os": "Debian GNU/Linux",
      "os_version": "11",
      "os_arch": "all",
      "purl": "pkg:deb/debian/ruby-thor@1.0.1-1?distro=11",
      "operator": "=",
      "affected": true
    }
  ]
}
```


ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.results[].name, .results[].version	Indicator.Attribute/ Vulnerability.Attribute	Affected Package	.results[].timelines. published_at	ruby-thor, version 1.0.1-1	User-configurable. Value composed from different attributes. Only ingested if the Product is affected and `Affected Products` is checked.

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.

With the **Save CVE Data As** parameter set to **Vulnerabilities**.

METRIC	RESULT
Run Time	3 minutes
Vulnerabilities	451
Vulnerability Attributes	49,350

Change Log

- **Version 1.1.1**
  - Added three new options to the **Ingested Context** configuration parameter: **Affected Products**, **Affected Libraries**, and **Affected Packages**. When these options are selected, the integration will make a call for this data via its supplemental feeds and ingest it into ThreatQ as attributes.
- **Version 1.1.0**
  - Updated the Flashpoint Ignite Vulnerabilities' endpoint.
  - Added support for Premium Flashpoint account attributes ingestion.
  - Added the following new parameters:
    - **Ingested Context** - select which pieces of context to ingest as attributes into ThreatQ.
    - **Premium Ingested Context** - select which pieces of context for Flashpoint Premium accounts to ingest as attributes into ThreatQ.
- **Version 1.0.1**
  - Added the following configuration options:
    - **Enable SSL Verification**
    - **Disable Proxies**
  - Resolved an issue where the fetching data from the provider would trigger an API timeout.
- **Version 1.0.0 rev-a**
  - Updated Integration name from **Flashpoint Ignite CDF** to **Flashpoint Ignite Vulnerabilities CDF**.
- **Version 1.0.0**
  - Initial release