ThreatQuotient

Metasploit Exploits CDF User Guide

Version 1.0.0

October 18, 2023

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	>= 4.22.0
Support Tier	ThreatQ Supported

Introduction

Metasploit is a very popular exploitation framework for building and executing exploits against known vulnerabilities. This feed consumes data from the public Metasploit code repository on Github about exploits published and available in the framework. The feed identifies the CVEs (where referenced) and can therefore be used for vulnerability prioritization. It is updated frequently and the recommended poll period for the source is daily.

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 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 **OSINT** 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 parameter under the **Configuration** tab:

PARAMETER	DESCRIPTION
Verify Host SSL	If checked, validates the server's certificate and checks whether the server's hostname matches. This parameter is enabled by 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

Metasploit Exploits

Sample Response:


```
{
    "auxiliary_admin/2wire/xslt_password_reset": {
        "name": "2Wire Cross-Site Request Forgery Password Reset
Vulnerability",
        "fullname": "auxiliary/admin/2wire/xslt_password_reset",
        "aliases": [],
        "rank": 300,
        "disclosure_date": "2007-08-15",
        "type": "auxiliary",
        "author": ["hkm <hkm@hakim.ws>", "Travis Phillips"],
        "description": "This module will reset the admin password on a 2Wire
wireless router.  This is\n        done by using the /xslt page where
authentication is not required, thus allowing\n        configuration changes
(such as resetting the password) as administrators.",
        "references": [
            "CVE-2007-4387",
            "OSVDB-37667",
            "BID-36075",
            "URL-https://seclists.org/bugtraq/2007/Aug/225"
        ],
        "platform": "",
        "arch": "",
        "rport": 80,
        "autofilter_ports": [80, 8080, 443, 8000, 8888, 8880, 8008, 3000,
8443],
        "autofilter_services": ["http", "https"],
        "targets": null,
        "mod_time": "2018-09-15 18:54:45 +0000",
        "path": "/modules/auxiliary/admin/2wire/xslt_password_reset.rb",
        "is_install_path": true,
        "ref_name": "admin/2wire/xslt_password_reset",
        "check": false,
        "post_auth": false,
        "default_credential": false,
        "notes": {}
    }
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.name	malware.value	N/A	.mod_time	2Wire Cross-Site Request Forgery Password Reset Vulnerability	
.description	malware.description	N/A	.mod_time	This module will reset the admin password on a 2Wire...	Mapped after some processing
N/A	malware.attribute	Type	.mod_time	Exploit	Hard coded
.references	malware.attribute	Reference URL	.mod_time	https://seclists.org/bugtraq/2007/Aug/225	Only if value starts with `URL-`
.references	malware.attribute	Reference	.mod_time	BID-36075	Excludes URL, CVE, and CWE refs
.references	malware.attribute	Disclosure Date	.mod_time	2007-08-15	
.author	malware.attribute	Author	.mod_time	Travis Phillips	
.references	vulnerability.value	N/A	.mod_time	CVE-2007-4387	Only if value starts with `CVE-`
.references	vulnerability.value	N/A	.mod_time	CWE-12345	Only if value starts with `CWE-`
N/A	vulnerability.attribute	Exploit Exists	.mod_time	True	Hard coded
N/A	vulnerability.attribute	Exploit in Metasploit	.mod_time	True	Hard coded
.references	indicator.value	CVE	.mod_time	CVE-2007-4387	Only if value starts with `CVE-`
N/A	indicator.attribute	Exploit Exists	.mod_time	True	Hard coded
N/A	indicator.attribute	Exploit in Metasploit	.mod_time	True	Hard coded

Change Log

- **Version 1.0.0**
  - Initial release