Outpost24

Vulnerability Management made easy

ServiceNow Integration

Version: 1.1

2018-06-20

Table of Contents

About This Guide

The purpose of this document is to provide users a comprehensive overview of the Outpost24 vulnerability scanner integration into ServiceNow.

For support information, visit https://www.outpost24.com/support.

Copyright

Trademark

1 Overview

1.1 Software Architecture Overview

The Outpost24 Vulnerability Integration is used to integrate ServiceNow with Outpost24 as a third-party vulnerability scanner. The scanner is created using the script include x_o24_outpost24. Outpost24Scanner provided by Outpost24 as an integration factory script. Any scan created in ServiceNow that use this scanner is sent to Outpost24 where the host is scanned. Vulnerabilities found are reported back to ServiceNow as vulnerable items.

1.2 Software Design Overview

The Outpost24Scanner script include extends VulnerabilityScannerBase and implements the functions `sendData` that sends a request to Outpost24 to start the scan and `retrieveData` that sends a request to Outpost24 to retrieve the status of the scan. The request to retrieve the status is sent every 5 minutes.

The application creates three scheduled script executions to import data from Outpost24 into ServiceNow. All scripts are implements paging to ensure that a limited set of data is sent in each request. The scripts are run on demand but can be configured to run at repeated intervals.

1.2.1 Compatibility Overview

Istanbul

1.3 Application Overview

- Import and populate Outpost24 asset data with ServiceNow DMDB data
- Enrich ServiceNow CMDB data with additional information if found
- Run Vulnerability scans from within ServiceNow

***Note**: English is the only supported language.*

2 System Requirements

Outpost24 Vulnerability Integration app requires the below mentioned modules in ServiceNow.

- Configuration Management Database (CMDB)
- Vulnerability Response
- System Import Sets

3 Setup and Configuration

3.1 Preparation for Installation

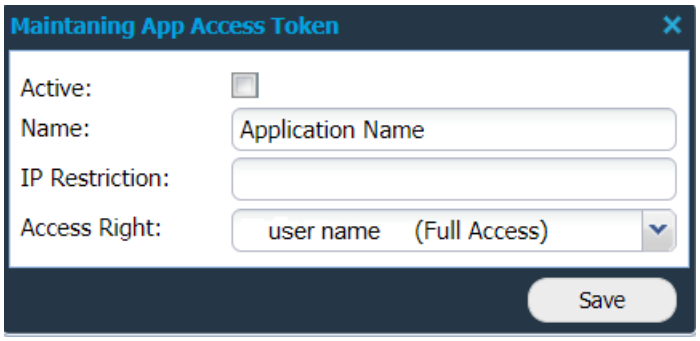
Before starting the setup:

1. Go to https://store.servicenow.com to download and install **Outpost24 Vulnerability Integration** app.
2. Log on with your credentials.

3.2 Setup

To setup and configure ServiceNow:

1. Go to Outpost24 **Vulnerability Management →Administration → Settings**.
2. Add the **API Server URL**; either OUTSCAN or HIAB to indicate which platform to use for scanning.
3. Add **API Access Token**; follow the below steps to generate an API Access Token from your OUTSCAN:
   a. Log on to **OUTSCAN**.
   b. Go to **Menu → Settings → Security Policy → Application Access Tokens**.
   c. Click **+New** to create a request.



   d. Fill in the required fields and click **Save**.
   e. This will generate an API Access token, which should be used in the respective application (**ServiceNow**).

4. Click **Save**.
5. Add **scanners** to OUTSCAN to use multiple scanners or internal scanners.

6. Go to **Vulnerability Scanning → Scanners**.
   a. Click **New** to add the Outpost24 vulnerability Scanner.
   b. Integration factory script must be new `x_o24_outpost24.Outpost24Scanner();` from the application **Outpost24 Vulnerability Integration**. This is automatically added while installing Outpost24 Vulnerability Integration app.
   c. After adding the required fields, click **Submit**.
   d. The added scanner will show up in the list of vulnerability scanners.

7. Add scan policies in OUTSCAN.
   ***Example**: A scan policy can set which credentials to use, vulnerabilities to look for and ports to scan.*

3.2.1 Add/Update Libraries

To add or update libraries:

1. Go to **Administration → Integrations**.
   a. Select Outpost24 – Import Vulnerability Scanners.
   b. All integrations are set to run **On Demand** as default. Change the frequency of update by selecting one of the options in the drop-down menu of **Run**.
   c. Click on **Execute Now** to run the script immediately.
   d. Click on **Update to save** the changes.

To update the **Scanners** immediately, go to **Libraries→Vulnerability Scanners**, click on **Refresh**.

2. Go to **Administration → Integrations**.
   a. Select Outpost24 – Import Vulnerability Database.
   b. To download Vulnerability Database, click on **Execute Now**.
   c. To keep the database up-to-date, change the update frequency to **Daily**.
   ***Note:** It is recommended to always update the database before running a scan.*

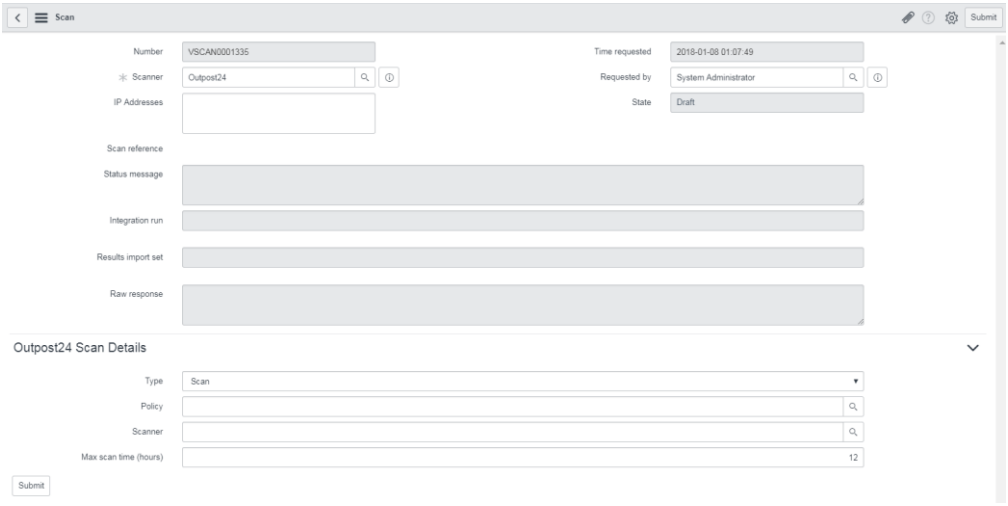
3. Go to **Administration → Integrations**.
   a. Select Outpost24 – Import Vulnerability Policies.
   b. To download Vulnerability policies, click on **Execute Now**.
   c. To keep the database up-to-date, change the update frequency to **Daily**.

To update the **Policies** immediately, go to **Libraries→Vulnerability Policies**, click on **Refresh**.

3.2.2 Run a scan

To run a scan:

1. Go to **Vulnerability Scanning → Scans**.
2. Click on **New** to add a scan schedule.



3. Add IP address(es) that are to be scanned.

3.2.2.1 Outpost24 Scan Details

1. **Type**: Select the scan type from the drop-down menu of **Type**.
   The available options are:
   - **Scan**
     - Select a **Policy** from the available options. Not mandatory.
     - Select a **Scanner**. Not mandatory.
     - Mention the **Max. scan time (hours)**.
   - **Discovery**
     - Select a **Scanner**. Not mandatory.
     - Mention the **Max. scan time (hours)**.
   - **SLS**
     - Select a **Scanner**. Not mandatory.
     - Mention the **Max. scan time (hours)**.
   - **Web**
     - Provide **URL(s)** that are to be scanned.
     - Select a **Scanner**. Not mandatory.
     - Mention the **Max. scan time (hours)**.

2. Click **Submit**. This will save the scan as a draft.
3. Go back to **Scans** window, click on the **Draft** scan to add a **configuration item** (if any).
   Note: *If IP address is delivered, the scan information is reported back to IP address. If* `sys_id` *is given,* OUTSCAN *fetches all information regarding connection (IP address, DNS hostname and FQDN) and the report will be sent to configuration item. If both are provided, then the IP address(es) mentioned is/are used as white list.*

4. Click on **Initiate scan**.

3.2.3 Scan Information

- To check if there are any errors, go to **Administration → Logs**.
- To see the scan history, go to **Management → Vulnerability Scanning → History**.
- Go to **Management → Vulnerabilities → Vulnerable Items**, click on the **Vulnerability** field on each ID to see the threat, and proposed solution.

Refer to *Integrations Guide* available in OUTSCAN/Support/Guides for information regarding how to enable ServiceNow on OUTSCAN.

4 Frequently Asked Questions

Which data and how is the data sent from scanners to ServiceNow?

ServiceNow → Outpost24

- Each configuration item's installed operating system and software components (for Outpost24 Scan-less Scanning SLS)
- Target network information (hostname, IP)

Outpost24 → ServiceNow

- Scanner metadata
- Scan policies
- Vulnerability database
- Detected findings

The data is transmitted via HTTPS.

How is SLS performed?

The operating system is fetched from the Configuration Item, name and version from installed_ons and sent in the RESTMessageV2 to the XMLAPI with parameters ACTION=SERVICENOWSCAN, SCANNER, SCANMODE, SCANPOLICY, MAXSCANTIME, and TARGETINFO.

OUTSCAN interprets this information and activates the vulnerability rule engine that generates findings based on which software components were submitted for the Configuration Item.

What volume have you tested and what is the speed at which they were imported? How does that compare to an existing large customer of yours (top 10% based on Configuration Items and Vulnerabilities)?

Our vulnerability database contains ~140000 items and is the largest dataset we attempted to import, the requests are however paged by 10000 in each request.

It appears that the response is read as a single String in memory. How large is the response anticipated to be? This can be a memory constraint that can affect our platform. If the response is XML or JSON our Datasource/import set/transform map implementation can step over results more efficiently in some cases. Also, this can be reduced by paging.

It depends on how many findings are detected on the scanned asset but the number of Vulnerable Items will typically range between a few and a few hundred.

Does this application import all vulnerability data from Outpost24 or does it only import results from scans initiated from within ServiceNow? How are Configuration Items matched from scan result data? We have some APIs for that but I don't see them used. If this is limited to scans initiated from ServiceNow this might not be important.

The application import results from scans initiated from within ServiceNow only, so this shouldn't be a concern.