Exporting Vulnerability Scanner Reports

In order to use the vulnerability sync feature, you will need to generate a report using your third-party vulnerability scanner. The following vendor reports are currently supported:

- CrowdStrike Falcon Spotlight - Vulnerability Report
- Rapid7 - Vulnerability Report Export
- Tenable - CSV Vulnerability Export

Requirements for the CSV import:

- The very first line in each CSV must contain this exact text: `hostname, cve id` .
- Hostnames are case-sensitive and must be an exact match to what is displayed in the Automox console.
  - Hostnames should not be wrapped in any quotes, parenthesis, brackets, or single tics.
- The CVE field should not contain any special characters other than dashes, for example CVE-2021-1234
- Severity is an optional field
  - Severities must use one of the following keywords: Critical, High, Medium, Low
- Hosts that have multiple CVEs to patch must be listed on individual lines.
- The CSV report must be less than 1 GB.

Example CSV file:

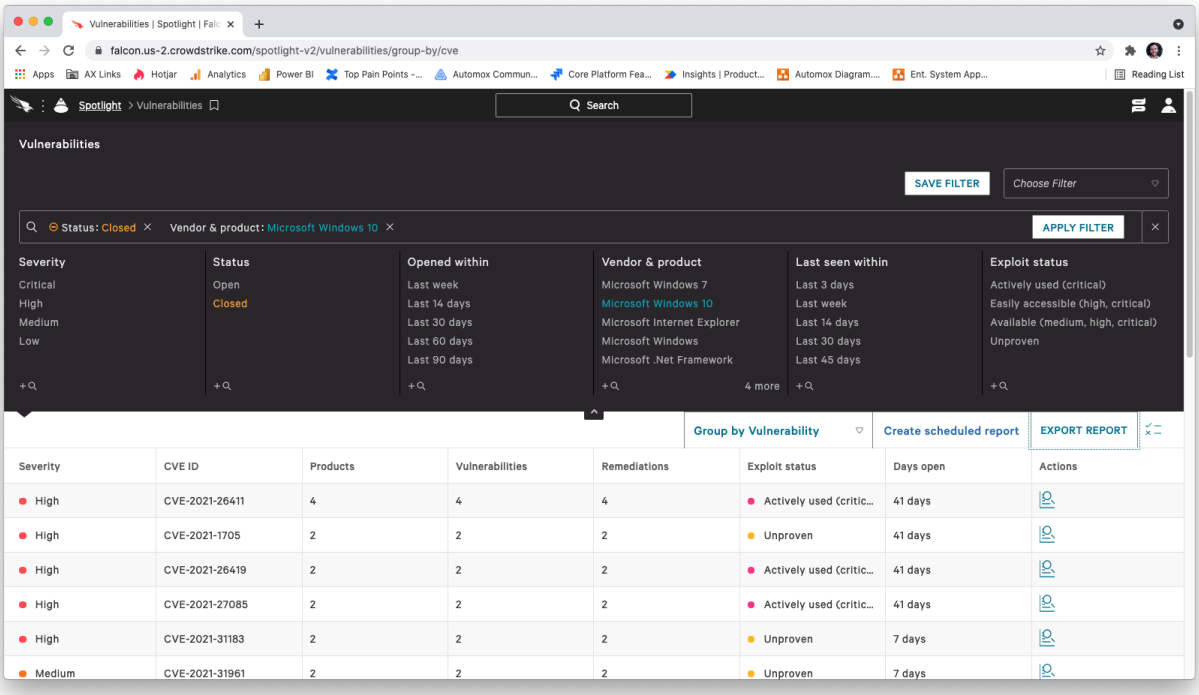
```
Hostname, CVE ID, Severity
finance-laptop,cve-2021-1234,high
finance-laptop,cve-2021-6789
finance-laptop,cve-2021-5522,critical
sales_laptop,cve-2021-9944,medium
```

Crowdstrike Falcon Spotlight - Vulnerability Report

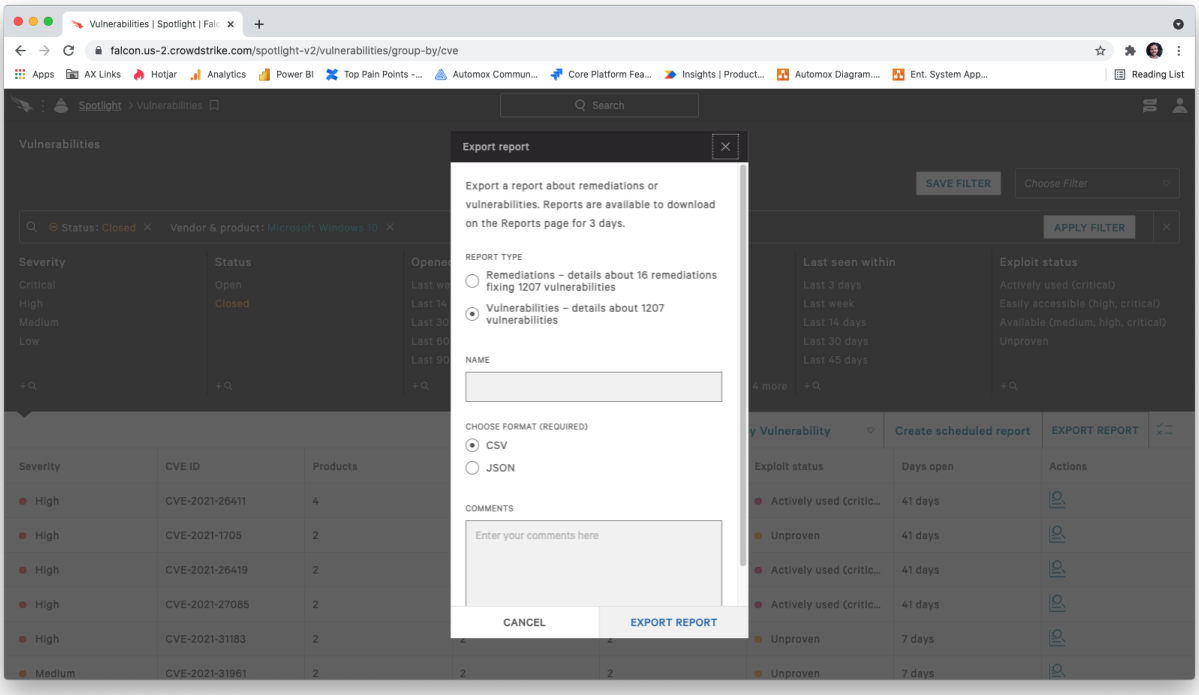
Follow these instructions to download a vulnerability report from the Crowdstrike Falcon Spotlight platform.

- From the Crowdstrike dashboard, ensure that the report identifies hostnames and CVE IDs.
- Be sure to include relevant filters as there is a file size limit for the ingest of 1 GB.
- Additionally, be aware that more CVE IDs will mean more tasks to be created by Automox.

Example of CrowdStrike's Spotlight Vulnerability Dashboard. **Note**: It is possible to filter on relevant vulnerabilities for the export.



- Select the file format CSV and export the report.



Rapid7 - Vulnerability Report Export

Follow these instructions to create and export a vulnerability report from the Rapid7 InsightVM/Nexpose platform.

Requirements: You must use the on-premise console to generate the report

Creating a Rapid7 vulnerability report

In order to easily export vulnerability findings from Rapid7 InsightVM/Nexpose in a format that is quickly imported into Automox, we recommend creating a Custom SQL Report. This can be done within the InsightVM console by following these steps:

1. Navigate to **Reports**.
2. On the Create a Report page, select **Export**.
3. Select **SQL Query Export** from the list of templates.
4. Add the query for the custom report and validate.
5. Save and run the report.

As new scans are performed, your Vulnerability Management team can regenerate reports and scope them to the groups, sites, and categories they are hoping to target. If the SQL query is modified for your environment needs, ensure the **hostname** and **cve id** fields are headers within the report export.

Query for custom SQL report

In the InsightVM/Nexpose Console, create a custom SQL Report using the following query:

```
select favf.asset_id, favf.vulnerability_id, da.host_name as hostname, dvf.reference as "cve id"
FROM fact_asset_vulnerability_finding favf
JOIN dim_vulnerability_reference dvf ON dvf.vulnerability_id = favf.vulnerability_id
JOIN dim_asset da ON da.asset_id = favf.asset_id
WHERE dvf.source = 'CVE'
```

That query will yield a result something like the following:

```
asset_id, vulnerability_id, hostname, cve id
18, 200, hostname-1, CVE-2017-8682
```

Make sure that it is saved in CSV format and use that file to upload into the console. Feel free to apply other filters to the SQL report. See also the following example queries for Rapid7 vulnerability reports:

Query for vulnerabilities with severity of Critical

This query is used to create a report for CVEs with a severity level of "critical".

```
select favf.asset_id, favf.vulnerability_id, da.host_name as hostname, dvf.reference as "cve id"
FROM fact_asset_vulnerability_finding favf
JOIN dim_vulnerability_reference dvf ON dvf.vulnerability_id = favf.vulnerability_id
JOIN dim_vulnerability dv ON favf.vulnerability_id = dv.vulnerability_id
JOIN dim_asset da ON da.asset_id = favf.asset_id
WHERE dvf.source = 'CVE' and dv.severity = 'Critical'
```

Query for vulnerabilities by specific CVEs

This query is used to create a report for a specific CVE.

```
select favf.asset_id, favf.vulnerability_id, da.host_name as hostname, dvf.reference as "cve id"
FROM fact_asset_vulnerability_finding favf
JOIN dim_vulnerability_reference dvf ON dvf.vulnerability_id = favf.vulnerability_id
JOIN dim_asset da ON da.asset_id = favf.asset_id
WHERE dvf.reference = 'CVE-1234'
```

If you need additional assistance or want to modify the query, use the Rapid7 documentation located here:

Creating reports based on SQL queries

Tenable - CSV Vulnerability Export

To download a vulnerability report from Tenable.io, follow the documentation as described here: Tenable Documentation: Export Vulnerability Data

Ensure that you apply the proper filters. The exported CSV report must include a column for CVE IDs and hostnames.