# Configuring JSON Support for the NVD Connector

## Overview

The National Vulnerability Database (NVD) would previously publish its list of vulnerabilities, known as Common Vulnerabilities and Exposures (CVE), in XML format through their CVE XML feed. Recently, the NVD introduced a JSON feed and announced their XML support would be end-of-life on October 9, 2019. As a result, customers must upgrade their NVD Connector to be compatible with the NVD JSON feed.

Starting September 9, 2019, the JSON 1.1 feed will be available for the NVD connector. Customers must download this feed to continue receiving vulnerability information from the JSON feed.

You must first upgrade the NVD Connector before upgrading to RiskVision version 9.3 or above. Upgrading an NVD connector includes access to the CPE Match Feed. The CPE Match Feed explicitly states which Common Platform Enumerators (CPE) are affected by which CVEs instead of just stating ranges of CPEs. The CPE Match Feed allows for increased accuracy when performing CPE matching.

The NVD patch will make the user's NVD Connector compatible with the JSON feed without upgrading the RiskVision server. Customers who do not upgrade their RiskVision server must apply the NVD patch. Contact the Resolver Support Team to receive the NVD path and installation instructions.

---

## Upgrade the NVD Connector

Unless otherwise stated, please remove the previous connector files.

1. Navigate to **C:\Program Files (x86)\Agiliance\NVD Connector\cfg** folder and back up the folder's contents.
2. Reinstall the NVD connector.
3. Open the **connector.file.properties** file and ensure it matches the file you backed up in step 1.
4. Set the following properties in the connector.file.properties file:

```
SupportedFormatExtensions = .xml,.json
```

```
cve.fromYear = [insert year connector should start importing datafeeds (e.g. 2002)]
```

- This property defaults to the year 2002, Resolver recommends you set it to the year before the current year.

```
cve.toYear = [insert year connector should stop importing datafeeds (e.g. 2019)]
```

- This defaults to the current year.

```
NvdCveUrl=https://nvd.nist.gov/feeds/json/cve/1.1/nvdcve-1.1-[YEAR].json.zip
```

- The `[YEAR]` property will pull in the year based on the range of the `cve.fromYear` and `cve.toYear` properties.
- If the `requestAutoFeed` property is `true`, the connector will contact the NVD website specified in the `NvdCveUrl` property and download the JSON files.
- If the property is `false`, any valid JSON file downloaded by the customer can be placed and immediately processed in the following location: **C:\Program Files (x86)\Agiliance\NVD Connector\data\connector.remote.cve\new**, allowing customers to download their CVE files.

```
NvdCpeMatchFeedURL=https://nvd.nist.gov/feeds/json/cpematch/1.0/nvdcpematch-1.0.json.zip
```

- An NVD connector configured for JSON will not run without the Match Feed provided by the above property.

5. Open the **File_wrapper.conf** file using **Notepad**.
6. Add a **Comment (#)** at the beginning of the **wrapper.java.maxmemory=1500** property.

```
#wrapper.java.maxmemory=1500
```

*Add Comment (#)*

7. Remove the **Comment (#)** from the beginning of the **wrapper.java.additional.1=** property and add **-Xmx10000m** to the end of the property.

```
wrapper.java.additional.1=-Xmx10000m
```

*Remove Comment (#)*

> ***Note:***
> *Users may need to increase their RAM by at least 500 MB to support this upgrade.*

8. Restart the NVD connector.
    - Press the **Windows + R** key on your keyboard.
    - From the ***Run*** pop-up, enter **services.msc** in the **Open** field.
    - Click the **OK** button or the **Enter** key.
    - From the ***Services*** screen, navigate to the **NVD Connector** on the **Services** list.
    - Click **NVD Connector**.
    - From the ***General*** tab on the ***Properties*** screen, click on the **Start** button under the ***Service Status*** section and click the **OK** button to stop the NDV Connector.
9. Forcefully update the pre-existing vulnerabilities CVSS scores when upgrading to RiskVision version 9.3 or above. This step does not apply to RiskVision versions 9.3 or lower, as those versions do not support CVSS v3.0 scores.
    - Disable the following RiskVision jobs before importing the NVD data:
        - Vulnerabilities Affected Entities Incremental Updates
        - Vulnerability Risk Score Calculator
        - Vulnerability Risk Score Initiator
        - Vulnerability Summary Update
        - Search Indexes Builder
    - Navigate to **%AGILIANCE_HOME%/config**.
    - Open the **agiliance.properties** file.
    - Set the following property to `true` :

      ```
      com.agiliance.agent.nvd.cve.forceUpdate
      ```

        - If this property is true, the NVD will only be updated if there is a difference between the vulnerability's published date in the JSON file and the vulnerability's published date in the database. Setting the property to true will bring CVSS v3.0 data for unchanged vulnerabilities.

> ***Note:***
> *CVSS 3.0 scores is **not** available before **12/20/2015**. For more details on CVSS, refer to the Vulnerability Metrics article here.*

10. Set the `com.agiliance.agent.nvd.cve.forceUpdate` property to `false` and resume the activities from step 9 once the CVSS values have been updated.

11. To re-authenticate the NVD Connector.
    - Open the Administration application in RiskVision.
    - Navigate to **Administration > Connectors**.
    - Click on the NVD Connector in the connectors list.
    - Under the Status section, click **Deny Access**.
    - Click **Authenticate**. NVD will now exclusively download JSON files rather than XML files.
12. When the import is complete, re-enable the jobs listed in step 9.