Vulnerability-CPE Matching

As part of CPE wild card search and matches, RiskVision has implemented a new property called **cpe.uri.regexp.criteria** to correlate all possible vulnerabilities that are applied to a specific CPE. By default, the property will take the **rightMatch** operator from the **version** and **update** columns and compile the rest with the **equalsMatch** operator. The property is shown below:

`cpe.uri.regexp.criteria=version:rightMatch::update_:rightMatch::edition:equalsMatch::language:equalsMatch::software_edition:equalsMatch::target_software:equalsMatch::t`

Each pair separated with **::** in the property value represents a column name and the SQL operator. The CPE match query will be prepared based on the above property value.

The system is not allowed to keep the partial property, therefore the user must provide the complete property in the **agiliance.properties** file.

The new property can be customized based on the matching criteria with the following supported operators:

- **rightMatch**
- **anyMatch**
- **equalsMatch**
- **leftMatch**
- **betweenMatch**

Version 2.3 of CPE is comprised of Well-Formed Name (WFN) components separated with ":" as below:

`cpe:2.3:part:vendor:product:version:update:edition:lang:sw_edition:target_sw:target_hw:other`

What follows are a few examples of using the CPE-Vulnerability matching using the wildcard.

CPEs associated with vulnerabilities processed in NVD input file:

Vuln1: **CVE-2021-27067** - cpe:2.3:o:microsoft:azure_devops_server:2019:update1:*:*:*:*:*:*

Vuln2: **CVE-2021-27089** - cpe:2.3:o:microsoft:windows_server_2008:r2:sp2:*:*:*:*:*:*

CPE exists in database without a vulnerability or without the above reported vulnerability:

CPE1: cpe:2.3:o:microsoft:azure_devops_server:2019.0.1:update1.1:*:*:*:*:*:*

CPE2: cpe:2.3:o:microsoft:azure_devops_server:2019.0.1:update1.2:*:*:*:*:*:*

CPE3: cpe:2.3:o:microsoft:windows_server_2008:r2:sp1:x64:*:*:*:*:*

Case 1: With default property (Version and Update with Right Match and rest are with Equal Match):

The vuln1, **CVE-2021-27067** with CPE **cpe:2.3:o:microsoft:azure_devops_server:2019:update1:*:*:*:*:*:*** will get matched to the following CPEs:

`cpe:2.3:o:microsoft:azure_devops_server:2019.0.1:update1.1:*:*:*:*:*:*`

`cpe:2.3:o:microsoft:azure_devops_server:2019.0.1:update1.2:*:*:*:*:*:*`

`cpe:2.3:o:microsoft:azure_devops_server:2019.0.2:update1.3:*:*:*:*:*:*`

Case 2: Version with Equal Match and rest are with Any Match:

The vuln1, CVE-2021-27067 with CPE cpe:2.3:o:microsoft:azure_devops_server:2019:update1:*:*:*:*:*:* will get matched to following CPEs:

`cpe:2.3:o:microsoft:azure_devops_server:2019:update1:*:*:*:*:*:*`

`cpe:2.3:o:microsoft:azure_devops_server:2019:update2:*:*:*:*:*:*`

`cpe:2.3:o:microsoft:azure_devops_server:2019`

`cpe:2.3:o:microsoft:azure_devops_server:2019:update1:XYZ:ABC*:*:*:*:*`

Case 3: All the components with Any Match:

The vuln1, CVE-2021-27067 with CPE cpe:2.3:o:microsoft:azure_devops_server:2019:update1:*:*:*:*:*:* will get matched to following CPEs

`cpe:2.3:o:microsoft:azure_devops_server:2019:update1:*:*:*:*:*:*`

`cpe:2.3:o:microsoft:azure_devops_server:2019:update2:*:*:*:*:*:*`

`cpe:2.3:o:microsoft:azure_devops_server:2019`

`cpe:2.3:o:microsoft:azure_devops_server:2019:update1:XYZ:ABC:*:*:*:*`

`cpe:2.3:o:microsoft:azure_devops_server:2020:update1:XYZ:ABC:*:*:*:*`

`cpe:2.3:o:microsoft:azure_devops_server:2021:update1:XYZ:ABC:*:*:*:*`

And vuln2, CVE-2021-27089 with CPE cpe:2.3:o:microsoft:windows_server_2008:r2:sp2:*:*:*:*:*:* will get matched to following CPEs

`cpe:2.3:o:microsoft:windows_server_2008:r2:sp1:x64:*:*:*:*:*`

`cpe:2.3:o:microsoft:windows_server_2008:r1:sp1:x64:*:*:*:*:*`

`cpe:2.3:o:microsoft:windows_server_2008:r2:sp2:x64:*:*:*:*:*`

The correlation of CPEs will be from NVD input file to Database.