Better <affected> Element

April 28th, 2008

MITRE

<affected> Element's Goal

Provide descriptive metadata about the products, platforms, and family that an OVAL Definition applies to.

MITRE

Version 5.4 <affected> Element

- details the specific system for which a definition has been written
- provides hints for tools using OVAL Definitions
  - help a reporting tool only use Windows definitions / preselect only Red Hat definitions
- inclusion of a particular platform/product does not mean the definition is physically checking for the existence of the platform or product

MITRE

Version 5.4 <affected> Element

- absence of the platform or product element can be thought of as definition applying to all platforms or products

- no restrictions on the platforms names that can be used
  - potentially leading to many different representations of the same value

MITRE

Version 5.4 Deficiencies

- Affected information is metadata only
  - Misleading
  - Unrelated to criteria
    - Family attribute may not align with criteria
    - Tendency to diverge from criteria
- Platform and product are unrelated
- Platform names are not standardized

MITRE

```
<definition id="oval:example:def:5" version="2" class="vulnerability">

    <metadata>
        <title>Word Memory Corruption Vulnerability</title>
        <affected family="windows">
            <platform>Microsoft Windows 2000</platform>
            <platform>Microsoft Windows XP</platform>
            <platform>Microsoft Windows Server 2003</platform>
            <product>Microsoft Word 2000</product>
            <product>Microsoft Word 2002</product>
            <product>Microsoft Word 2003</product>
        </affected>
        <reference ref_id="CVE-1234-5678" ref_url="http://cve.mitre.org/cve.cgi?name=CVE-1234-5678" source="CVE"/>
        <description>Some nice description here... description>
    </metadata>

    <criteria operator="OR">
        <criteria operator="AND">
            <extend_definition comment="Microsoft Word 2000 is installed" definition_ref="oval: example:def:455"/>
            <criterion comment="the version of Winword.exe is less than 9.0.0.8966" test_ref="oval: example:tst:7689"/>
        </criteria>
        <criteria operator="AND">
            <extend_definition comment="Microsoft Word 2002 is installed" definition_ref="oval: example:def:973"/>
            <criterion comment="the version of Winword.exe is less than 10.0.6838.0" test_ref="oval: example:tst:7432"/>
        </criteria>
        <criteria operator="AND">
            <extend_definition comment="Microsoft Word 2003 is installed" definition_ref="oval: example:def:475"/>
            <criterion comment="the version of Winword.exe is less than 11.0.8202.0" test_ref="oval: example:tst:7773"/>
        </criteria>
    </criteria>

</definition>
```

Version 6 Requirements

- Directly relate affected information to the evaluated criterion of a definition.
- Support selecting sets of applicable definitions for a system.
- Provide suitable metadata for UI display.
- Support standardized platform names.

MITRE

Version 6 Proposal

- Drop existing affected element
- Add a new type of <affected> criterion
  - Resembles the existing <extend_definition> criterion
  - Includes a CPE reference
- Affected information is embedded in each definition's criteria

MITRE

```
<definition id="oval:example:def:2" version="2" class="vulnerability">

    <metadata>
        <title>Word Memory Corruption Vulnerability</title>
        <reference ref_id="CVE-1234-5678" ref_url="http://cve.mitre.org/name.cgi?name=CVE-1234-5678" source="CVE"/>
        <description>Some nice description here.</description>
    </metadata>

    <criteria operator="OR">

        <criteria operator="AND">
            <!-- affected application -->
            <affected cpe_id="cpe:/a:microsoft:word:2000" comment="Microsoft Word 2000 is installed“
                      definition_ref="oval:example:def:4"/>
            <criterion comment="the version of Winword.exe is less than 9.0.0.8966" test_ref="oval:example:tst:1"/>
        </criteria>

        <criteria operator="AND">
            <!-- affected application -->
            <affected cpe_id="cpe:/a:microsoft:word:2002" comment="Microsoft Word 2002 is installed"
                      definition_ref="oval:example:def:5"/>
            <criterion comment="the version of Winword.exe is less than 10.0.6838.0" test_ref="oval:example:tst:2"/>
        </criteria>

        <criteria operator="AND">
            <!-- affected application -->
            <affected cpe_id="cpe:/a:microsoft:office:2003" comment="Microsoft Word 2003 is installed"
                      definition_ref="oval:example:def:6"/>
            <criterion comment="the version of Winword.exe is less than 11.0.8202.0" test_ref="oval:example:tst:3"/>
        </criteria>

    </criteria>

</definition>
```

Discussion

- Affected information is:
  - conveyed through criteria and based on inventory definitions
  - still readily available for UI display
  - tied to CPE Names
  - must be encoded in the criteria of a definition
    - causes duplication in definition criterion
- No distinction is made between affected family, operating system, or platform.

MITRE

Discussion

- Family information does not align with CPE.
  - This change will drop the notion of family from affected metadata.
  - The <family_test> will remain in OVAL since it serves a different purpose.

- CPE Name parsing may be required when preselecting sets of definitions.
  - Selecting all Microsoft OS definitions will require looking for “cpe:/o:microsoft:”.

MITRE