Qualys Cloud Platform v3.x

API Release Notes

Version 3.4

November 30, 2020

Qualys Cloud Suite API gives you many ways to integrate your programs and API calls with Qualys capabilities. You'll find all the details in our user guides, available at the time of release. Just log in to your Qualys account and go to Help > Resources.

What's New

WAS API: Finding Output to Identify Potential Vulnerability and Show Original QID Severity

WAS API: WAS Scan Download to Show Severity, Original Severity, and Potential Information

MDS API: Search and View Detection Output to Include associated WAS Web App ID

URL to the Qualys API Server

The Qualys API URL you should use for API requests depends on the Qualys platform where your account is located.

Click here to identify your Qualys platform and get the API URL

This documentation uses the API gateway URL for Qualys US Platform 1 (https://gateway.qg1.apps.qualys.com) in sample API requests. If you're on another platform, please replace this URL with the appropriate gateway URL for your account.

WAS API: Finding Output to Identify Potential Vulnerability and Show Original QID Severity

API affected	/qps/rest/2.0/search/was/finding /qps/rest/2.0/get/was/finding/<id>
New or Updated APIs	Updated
DTD or XSD changes	Yes

The Search and Get Findings API output contains category to distinguish between Vulnerability, Sensitive Content and Information Gathered. However, these categories do not have a field to specify if findings for a vulnerability is confirmed or potential. We added a new parameter <potential> in the API output to display this information. Findings for the potential vulnerability show potential as true, and findings for the confirmed vulnerability show potential as false.

Also, the output do not mention the original severity of the QID (if the severity is edited from the KnowledgeBase) or finding (if the finding severity is edited from detection list). We added a new parameter <originalSeverity> in the API output to show the original severity for the edited QIDs from the Knowledgebase/finding.

New fields are shown for Vulnerability, Sensitive Content, and Information Gathered categories.

Permissions

- You must have the WAS module enabled.

- You must have the "API access" and "Access WAS module" permissions.

Sample - Get details of a finding

The finding details show the new potential parameter.

API Request

```
curl -u "USERNAME:PASSWORD" -H "content-type: text/xml" -X "GET" --
"https://qualysapi.qualys.com/qps/rest/3.0/get/was/catalog/f717f2db-c6bb-
426f-ba80-f3617432317f"
```

XML Output

```
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xsd/3.0/w
as/finding.xsd">
    <responseCode>SUCCESS</responseCode>
    <count>1</count>
    <data>
```

```
        <Finding>
            <id>2864786</id>
            <uniqueId>f717f2db-c6bb-426f-ba80-f3617432317f</uniqueId>
            <qid>38170</qid>
            <name>
                <![CDATA[SSL Certificate - Subject Common Name Does Not
Match Server FQDN]]>
            </name>
            <type>VULNERABILITY</type>
            <potential>true</potential>
            <findingType>QUALYS</findingType>
            <group>INFO</group>
            <resultList>
                <count>1</count>
                <list>
                    <Result>
                        <payloads>
                            <count>0</count>
                        </payloads>
                    </Result>
                </list>
            </resultList>
            <severity>2</severity>
            <url>
                <![CDATA[http://w2ksrv-remedy1.vuln.qa.qualys.com:443/]]>
            </url>
            <status>ACTIVE</status>
            <firstDetectedDate>2020-07-27T22:50:35Z</firstDetectedDate>
            <lastDetectedDate>2020-11-15T11:44:51Z</lastDetectedDate>
            <lastTestedDate>2020-11-15T11:44:51Z</lastTestedDate>
            <timesDetected>30</timesDetected>
            <webApp>
                <id>5436796</id>
                <name>
                    <![CDATA[Catalog Web Application: w2ksrv-
remedy1.vuln.qa.qualys.com, Port 443]]>
                </name>
                <url>
                    <![CDATA[http://w2ksrv-
remedy1.vuln.qa.qualys.com:443/]]>
                </url>
                <tags>
                    <count>0</count>
                </tags>
            </webApp>
            <isIgnored>false</isIgnored>
            <sslData>
                <flags>v</flags>
                <protocol>tcp</protocol>
```

```
                <virtualhost>w2ksrv-
remedy1.vuln.qa.qualys.com</virtualhost>
                <ip>10.10.10.222</ip>
                <port>443</port>
                <result>
                    <![CDATA[Certificate #0 CN=w2ksrv-remedy1.w3ktest-
1.vuln.qa.qualys.com,O=Trend_Micro_internal_CA (w2ksrv-remedy1.w3ktest-
1.vuln.qa.qualys.com) and (w2ksrv-remedy1.vuln.qa.qualys.com) don't match
]]>
                </result>
                <sslDataInfoList>
                    <list>
                        <SSLDataInfo>

<certificateFingerprint>41BA2F3826788BE78ACA5CEE72516C5ED4507B9C2C8AB1EF2
A8AEF6ECD5CB954</certificateFingerprint>
                            <sslDataCipherList/>
                            <sslDataKexList/>
                            <sslDataPropList/>
                        </SSLDataInfo>
                    </list>
                </sslDataInfoList>
            </sslData>
        </Finding>
    </data>
</ServiceResponse>
```

Sample - Search a finding

Let us search a finding to view the finding potential and original severity.

API Request

```
curl -u "USERNAME:PASSWORD" -H "content-type: text/xml" -X "POST" --
data-binary @-
"https://qualysapi.qualys.com/qps/rest/3.0/search/was/finding/" <
file.xml
Note: "file.xml" contains the request POST data.
```

Request POST data

```
<ServiceRequest>
    <filters>
        <Criteria field="uniqueId" operator="EQUALS">4e3bc54c-565f-4dd6-
9e97-92572ddb0ded</Criteria>
    </filters>
</ServiceRequest>
```

XML Output

```
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xsd/3.0/w
as/finding.xsd">
    <responseCode>SUCCESS</responseCode>
    <count>1</count>
    <hasMoreRecords>false</hasMoreRecords>
    <data>
        <Finding>
            <id>631251</id>
            <uniqueId>4e3bc54c-565f-4dd6-9e97-92572ddb0ded</uniqueId>
            <qid>6</qid>
            <name>
                <![CDATA[DNS Host Name]]>
            </name>
            <type>INFORMATION_GATHERED</type>
            <potential>false</potential>
            <findingType>QUALYS</findingType>
            <resultList>
                <count>1</count>
                <list>
                    <Result>
                        <authentication>false</authentication>
                        <payloads>
                            <count>0</count>
                        </payloads>
                    </Result>
                </list>
            </resultList>
            <severity>5</severity>
            <originalSeverity>1</originalSeverity>
            <firstDetectedDate>2020-05-19T12:40:26Z</firstDetectedDate>
            <lastDetectedDate>2020-05-19T12:40:26Z</lastDetectedDate>
            <lastTestedDate>2020-05-19T18:33:40Z</lastTestedDate>
            <webApp>
                <id>4850671</id>
                <name>
                    <![CDATA[SD Dashboard app]]>
                </name>
                <url>
                    <![CDATA[http://10.11.72.39]]>
                </url>
                <tags>
                    <count>1</count>
                    <list>
                        <Tag>
                            <id>9358139</id>
```

```
                            <name>
                                <![CDATA[Tag1 1582696957250]]>
                            </name>
                        </Tag>
                    </list>
                </tags>
            </webApp>
        </Finding>
    </data>
</ServiceResponse>
```

Updated XSD

<platform API server>/qps/xsd/3.0/was/finding.xsd

We added two new elements "`potential`" and "`originalSeverity`" in the finding.xsd.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
    ...
     </xs:element>
           <xs:element name="potential" minOccurs="0" type="xs:boolean"/>
            <xs:element name="findingType" minOccurs="0">
                <xs:simpleType>
                    <xs:restriction base="xs:string">
                         ...
                         <xs:element name="resultList" type="ResultList"
minOccurs="0"  />
 <xs:element name="severity" type="xs:string" minOccurs="0"/>
            <xs:element name="originalSeverity" type="xs:string"
minOccurs="0"/>
          <xs:element name="url" type="Url" minOccurs="0"/>
<xs:element name="status" minOccurs="0">
<xs:simpleType>
...
```

WAS API: WAS Scan Download to Show Severity, Original Severity, and Potential Information

API affected	/qps/rest/3.0/download/was/wascan/{id}
New or Updated APIs	Updated
DTD or XSD changes	Yes

The WAS Scan API output displays findings in WasScanVuln, WasScanSensitiveContent, and WasScanIg tags. These three tags contain finding details of every category; however, we do not specify if the finding for a vulnerability is confirmed or potential. Also, we do not mention the severity of a QID and original severity in case the severity is edited by the user from the KnowledgeBase.

We added <severity> and <originalSeverity> parameters in the WasScanVuln, WasScanSensitiveContent, and WasScanIg tags to show the severity and original severity of the vulnerability and added <potential> parameter to WasScanVuln tag. For the potential vulnerability, the <potential> parameter will show potential true and for confirmed vulnerability, this parameter will show potential false.

Permissions

- You must have the WAS module enabled.

- You must have the "API access" and "Access WAS module" permissions.

- You must have "WAS.SCAN.READ".

Sample - Download Scan

API Request

```
curl -u "USERNAME:PASSWORD" -H "content-type: text/xml" -X "GET" --
"https://qualysapi.qualys.com/qps/rest/3.0/download/was/wasscan/3616350"
```

XML Output

```
<?xml version="1.0" encoding="UTF-8"?>
<?xml version="1.0" encoding="UTF-8"?>
<WasScan xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xsd/3.0/w
as/wasscan.xsd">
    <id>3616350</id>
    <name>
        <![CDATA[Relaunch 2020-09-29 5:43:56PM]]>
    </name>
    <reference>was/1601381644899.920367</reference>
    <type>VULNERABILITY</type>
    ...
```

```
                <WasScanVuln>
                    <qid>150004</qid>
                    <severity>3</severity>
                    <originalSeverity>2</originalSeverity>
                    <potential>false</potential>
                    <title>
                        <![CDATA[Path-Based Vulnerability]]>
                    </title>
                    <uri>
                        <![CDATA[http://10.11.72.39/includes/]]>
                    </uri>
                    <instances>
                        <count>1</count>
                        <list>
                            <WasScanVulnInstance>
                                <authenticated>false</authenticated>
                                <payloads>
                                    <count>1</count>
                                    <list>
                                        <WasScanVulnPayload>
                                            <payload>

<![CDATA[http://10.11.72.39/includes/]]>
                                            </payload>
                                            <result base64="true">

<![CDATA[Y29tbWVudDogVGhlIHNlcnZlciByZXNwb25kZWQgd2l0aCBhIHZlcmJvc2UgZXJy
b3IgbWVzc2FnZSBmb3IgdGhpcyByZXF1ZXN0LgpIVFRQLzEuMSA0MDMgRm9yYmlkZGVu]]>
                                            </result>
                                        </WasScanVulnPayload>
                                    </list>
                                </payloads>
                            </WasScanVulnInstance>
                        </list>
                    </instances>
                </WasScanVuln>
...
```

Updated XSD

<platform API server>/qps/xsd/3.0/was/wasscan.xsd

We added new child elements "severity" and "originalSeverity" under the elements: WasScanVuln, WasScanSensitiveContent, and WasScanIg and also added the child element "potential" under "WasScanVuln" in the wasscan.xsd.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
```

```
    elementFormDefault="qualified">

    <!-- REQUEST -->
    <xs:element name="ServiceRequest">
        <xs:complexType>
            <xs:all>
                <xs:element name="filters" type="ServiceRequestFilters"
minOccurs="0"/>
                <xs:element name="preferences"
type="ServiceRequestPreferences" minOccurs="0"/>
                <xs:element name="data" type="ServiceRequestData"
minOccurs="0"/>
            </xs:all>
        </xs:complexType>
    </xs:element>
...
    <xs:complexType name="WasScanVuln">
        <xs:all>
            <xs:element name="qid" type="xs:long" />
            <xs:element name="severity" type="xs:string" />
            <xs:element name="originalSeverity" type="xs:string" />
            <xs:element name="potential" type="xs:boolean" />
            <xs:element name="title" type="Cdata" />
            <xs:element name="uri" type="Url" />
            <xs:element name="param" type="xs:string" minOccurs="0"/>
           <xs:element name="instances" type="WasScanVulnInstanceList" />
            <xs:element name="sslData" type="SSLData" minOccurs="0" />
        </xs:all>
    </xs:complexType>
...
    <xs:complexType name="WasScanSensitiveContent">
        <xs:all>
            <xs:element name="qid" type="xs:string" />
            <xs:element name="severity" type="xs:string" />
            <xs:element name="originalSeverity" type="xs:string" />
            <xs:element name="title" type="Cdata" />
            <xs:element name="uri" type="Url" />
            <xs:element name="param" type="xs:string" minOccurs="0"/>
            <xs:element name="content" type="xs:string" minOccurs="0"/>
            <xs:element name="instances"
type="WasScanSensitiveContentInstanceList" />
            <xs:element name="sslData" type="SSLData" minOccurs="0" />
        </xs:all>
    </xs:complexType>
...
    <xs:complexType name="WasScanIg">
        <xs:all>
            <xs:element name="qid" type="xs:long" />
            <xs:element name="severity" type="xs:string" />
```

```
        <xs:element name="originalSeverity" type="xs:string" />
        <xs:element name="title" type="Cdata" />
        <xs:element name="data" type="Base64Data" />
        <xs:element name="sslData" type="SSLData" minOccurs="0" />
    </xs:all>
</xs:complexType>
```

MDS API: Search and View Detection Output to Include associated WAS Web App ID

API affected	/qps/rest/1.0/search/md/detection /qps/rest/1.0/get/md/detection/{id}
New or Updated APIs	Updated
DTD or XSD changes	Yes

We now show two new parameters <siteid> (site ID) and <wasid> (web applicaiton ID) for malware detections in the Search detections and View malware detection details output. This information links a detection back to the WAS application for which detection is made. Web application ID is shown only if the site is controlled by the WAS application. In this case only site ID is shown.

In the View malware detection details output we show asset Id which is same as site ID and web application ID if the site is controlled by the WAS application.

Sample - Search detections

API Request

```
curl -u "USERNAME:PASSWORD" -H "content-type: text/xml" -X "POST" --
data-binary @-
"https://qualysapi.qualys.com/qps/rest/1.0/search/md/detection/" <
file.xml
Note: "file.xml" contains the request POST data.
```

Request POST data

```
<ServiceRequest>
    <preferences>
        <limitResults>100</limitResults>
    </preferences>
    <filters>
        <Criteria field="type" operator="EQUALS">STATIC</Criteria>
    </filters>
</ServiceRequest>
```

XML Output

```
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xsd/1.0/m
d/detection.xsd">
    <responseCode>SUCCESS</responseCode>
    <count>6</count>
    <hasMoreRecords>false</hasMoreRecords>
```

```
    <data>
        <Detection>
            <id>430627016</id>
            <qid>207400</qid>
            <name>
                <![CDATA[HTTP 4xx Error]]>
            </name>
            <type>STATIC</type>
            <severity>LOW</severity>
            <url>
                <![CDATA[https://sdm-
gallery.ru/exibitions/204/%20/upload/iblock/76a/76a6e0333ca5d26dab9a048e7
69b55ff.pdf]]>
            </url>
            <siteId>63092273</siteId>
        </Detection>
        <Detection>
            <id>430637019</id>
            <qid>207400</qid>
            <name>
                <![CDATA[HTTP 4xx Error]]>
            </name>
            <type>STATIC</type>
            <severity>LOW</severity>
            <url>
                <![CDATA[https://sdm-
gallery.ru/exibitions/204/%20/upload/iblock/76a/76a6e0333ca5d26dab9a048e7
69b55ff.pdf]]>
            </url>
            <siteId>63094273</siteId>
            <wasId>63091274</wasId>
        </Detection>
    </data>
</ServiceResponse>
```

Sample - View malware detection details

API Request

```
curl -u "USERNAME:PASSWORD" -X "GET"
"https://qualysapi.qualys.com/qps/rest/1.0/get/md/detection/"
```

XML Output

```
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xsd/1.0/m
d/detection.xsd">
    <responseCode>SUCCESS</responseCode>
    <count>1</count>
```

```
    <data>
        <Detection>
            <id>430637019</id>
            <qid>207400</qid>
            <name>
                <![CDATA[HTTP 4xx Error]]>
            </name>
            <type>STATIC</type>
            <severity>LOW</severity>
            <url>
                <![CDATA[https://sdm-
gallery.ru/exibitions/204/%20/upload/iblock/76a/76a6e0333ca5d26dab9a048e7
69b55ff.pdf]]>
            </url>
            <asset>
                <id>63094273</id>
                <name>
                    <![CDATA[http://10.115.51.102]]>
                </name>
                <deactivated>false</deactivated>
                <wasId>63091274</wasId>
            </asset>
        </Detection>
    </data>
</ServiceResponse>
```

Updated XSD

<platform API server>/qps/xsd/1.0/md/detection.xsd

We added two new child elements "siteId" and "wasId" under "Detection" element.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    elementFormDefault="qualified">
    <!-- REQUEST -->
    <xs:element name="ServiceRequest">
        <xs:complexType>
            <xs:all>
                <xs:element name="filters" type="ServiceRequestFilters"
minOccurs="0"/>
                <xs:element name="preferences"
type="ServiceRequestPreferences" minOccurs="0"/>
                <xs:element name="data" type="ServiceRequestData"
minOccurs="0"/>
            </xs:all>
        </xs:complexType>
    </xs:element>
```

```
    <xs:complexType name="ServiceRequestFilters">
      <xs:sequence>
        <xs:element name="Criteria" type="Criteria"
maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>

    <xs:complexType name="Criteria">
      <xs:simpleContent>
       <xs:extension base="xs:string">
          <xs:attribute name="field" type="xs:string"/>
          <xs:attribute name="operator">
              <xs:simpleType>
                    <xs:restriction base="xs:string">
                        <xs:enumeration value="CONTAINS"/>
                        <xs:enumeration value="IN"/>
                        <xs:enumeration value="EQUALS"/>
                        <xs:enumeration value="NOT EQUALS"/>
                        <xs:enumeration value="GREATER"/>
                        <xs:enumeration value="LESSER"/>
                        <xs:enumeration value="NONE"/>
                    </xs:restriction>
                </xs:simpleType>
                </xs:attribute>
       </xs:extension>
      </xs:simpleContent>
    </xs:complexType>

    <xs:complexType name="ServiceRequestPreferences">
      <xs:all>
        <xs:element name="startFromId" type="xs:long" minOccurs="0"/>
        <xs:element name="startFromOffset" type="xs:int" minOccurs="0"/>
        <xs:element name="limitResults" type="xs:int" minOccurs="0"/>
        </xs:all>
    </xs:complexType>

    <xs:complexType name="ServiceRequestData">
      <xs:sequence>
        <xs:element name="Detection" type="Detection" minOccurs="0"/>
        </xs:sequence>
    </xs:complexType>


    <!-- RESPONSE -->
    <xs:element name="ServiceResponse">
        <xs:complexType>
            <xs:sequence>
            <xs:element name="responseCode" type="ResponseCode"/>
```

```
        <xs:element name="responseErrorDetails"
         type="ResponseErrorObject" minOccurs="0"/>
        <xs:element name="count" type="xs:int" minOccurs="0"/>
        <xs:element name="hasMoreRecords" type="xs:boolean"
        minOccurs="0"/>
        <xs:element name="lastId" type="xs:long" minOccurs="0"/>
        <xs:element name="data" type="ServiceResponseData"
        minOccurs="0"/>
        </xs:sequence>
    </xs:complexType>
</xs:element>

<xs:simpleType name="ResponseCode">
    <xs:restriction base="xs:string">
        <xs:enumeration value="AUTH_CREDENTIALS_NEEDED"/>
        <xs:enumeration value="CANNOT_BE_NULL"/>
        <xs:enumeration value="INVALID_XML"/>
        <xs:enumeration value="INVALID_CREDENTIALS"/>
        <xs:enumeration value="INVALID_API_VERSION"/>
        <xs:enumeration value="INVALID_PARAM"/>
        <xs:enumeration value="INVALID_URL"/>
        <xs:enumeration value="INVALID_REQUEST"/>
        <xs:enumeration value="NOT_FOUND"/>
        <xs:enumeration value="OTHER_ERROR"/>
        <xs:enumeration value="OPERATION_NOT_SUPPORTED"/>
        <xs:enumeration value="EVALUATION_EXPIRED"/>
        <xs:enumeration value="JMS_SERVER_DOWN"/>
        <xs:enumeration value="RMI_SERVER_DOWN"/>
        <xs:enumeration value="SUCCESS"/>
        <xs:enumeration value="STILL_PROCESSING"/>
        <xs:enumeration value="UNAUTHORIZED"/>
        <xs:enumeration value="UNAUTHORIZED_DESTINATION_APPS"/>
        <xs:enumeration value="UNIDENTIFIED_PRODUCER"/>
        <xs:enumeration value="UNKNOWN_OBJECT"/>
    </xs:restriction>
</xs:simpleType>

<xs:complexType name="ResponseErrorObject">
  <xs:sequence>
    <xs:element name="errorMessage" type="xs:string"/>
    <xs:element name="errorResolution" type="xs:string"
     minOccurs="0"/>
    <xs:element name="internalErrorCodeId" type="xs:int"
     minOccurs="0"/>
  </xs:sequence>
</xs:complexType>

<xs:complexType name="ServiceResponseData">
    <xs:sequence>
```

```
            <xs:element ref="Detection" minOccurs="0"
               maxOccurs="unbounded" />
         </xs:sequence>
     </xs:complexType>


     <!-- DATA -->
     <xs:element name="Detection" type="Detection" />

     <xs:complexType name="Detection">
    <xs:all>
       <xs:element name="id" type="xs:long" minOccurs="1" maxOccurs="1" />
    <xs:element name="qid" type="xs:long" minOccurs="1" maxOccurs="1" />
       <xs:element name="name" type="Cdata" minOccurs="1" maxOccurs="1" />
    <xs:element name="type" type="DetectionType" minOccurs="1"
maxOccurs="1" />
   <xs:element name="description" type="Cdata" minOccurs="0" maxOccurs="1"
/>
   <xs:element name="severity" type="Severity" minOccurs="0" maxOccurs="1"
/>
    <xs:element name="url" type="Url" minOccurs="0"/>
    <xs:element name="result" type="Cdata" minOccurs="0" />
    <xs:element name="asset" type="Asset" minOccurs="0"/>
  <xs:element name="siteId" type="xs:long" minOccurs="1" maxOccurs="1" />
    <xs:element name="wasId" type="xs:long" minOccurs="0" />
    </xs:all>
</xs:complexType>

<xs:complexType name="Cdata">
       <xs:simpleContent>
           <xs:extension base="xs:string"/>
       </xs:simpleContent>
    </xs:complexType>

<xs:simpleType name="DetectionType">
<xs:restriction base="xs:string">
<xs:enumeration value="STATIC" />
            <xs:enumeration value="BEHAVIORAL" />
            <xs:enumeration value="ANTIVIRUS" />
            <xs:enumeration value="REPUTATION" />
            <xs:enumeration value="MISC" />
</xs:restriction>
</xs:simpleType>

<xs:simpleType name="Severity">
<xs:restriction base="xs:string">
<xs:enumeration value="HIGH" />
            <xs:enumeration value="MEDIUM" />
            <xs:enumeration value="LOW" />
```

```
</xs:restriction>
</xs:simpleType>

<xs:complexType name="Url">
        <xs:simpleContent>
            <xs:extension base="Cdata"/>
        </xs:simpleContent>
    </xs:complexType>

    <xs:complexType name="Asset">
       <xs:all>
           <xs:element name="id" type="xs:long" minOccurs="0"/>
           <xs:element name="name" type="Cdata" minOccurs="0"/>
           <xs:element name="url" type="Url" minOccurs="0"/>
           <xs:element name="deactivated" type="xs:boolean"
minOccurs="0"/>
           <xs:element name="wasId" type="xs:long" minOccurs="0" />
       </xs:all>
    </xs:complexType>

</xs:schema>
```