Qualys Cloud Platform (VM, PC) v10.x

API Release Notes

Version 10.23

July 24, 2023

This new version of the Qualys Cloud Platform (VM, PC) includes improvements to the Qualys API. 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

Renamed ARS-Related Parameters to Replace ARS with TruRisk

Enhanced Host Details

Introduced Unique IDs for Vulnerability Detections

Qualys API Server URL

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

Renamed ARS-Related Parameters to Replace ARS with TruRisk

With this release, all the ARS (Asset Risk Score) related parameters are renamed to replace ARS with TruRisk in the List Hosts API and the host-based scan reports, both XML and CSV formats.

Important: The old parameters with ARS will be retained for the next few releases. However, there will be a future update where these parameters will be removed with advance notification.

The following APIs have been updated:

List Hosts

Download Saved Reports

List Hosts

APIs affected	/api/2.0/fo/asset/host/?action=list
New or Updated API	Updated
DTD or XSD changes	Yes

With this release, all the ARS (Asset Risk Score) related parameters are renamed to replace ARS with TruRisk score.

Important: The old parameters with ARS will be retained for the next few releases. However, there will be a future update where these parameters will be removed with advance notification.

Input Parameters

The following input parameters are renamed:

Old Parameter	Renamed Parameter	Description
show_ars={0|1}	show_trurisk={0|1}	Specify 1 to show the TruRisk score in the output.
ars_min={value}	trurisk_min={value}	Show only asset records with a TruRisk value greater than or equal to the TruRisk min value specified. The trurisk_min can only be specified when show_trurisk=1. When trurisk_min and trurisk_max are specified in the same request, the trurisk_min value must be less than the trurisk_max value.
ars_max={value}	trurisk_max={value}	Show only detection records with a TruRisk value less than or equal to the TruRisk max value specified. The trurisk_max can only be specified when show_trurisk=1. When trurisk_min and trurisk_max are specified in the same request, the trurisk_min value must be less than the trurisk_max value.
show_ars_factors={0|1}	show_trurisk_factors={0|1}	Specify 1 to show TruRisk contributing factors associated with each asset record in the output.

API Sample

Sample - List Host Assets with TruRisk Score

API Request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl"
"<qualys_base_url>/api/2.0/fo/asset/host/action=list&ips=10.21.31.41&show
_trurisk=1&trurisk_min=0&trurisk_max=1000&show_trurisk_factors=1"
```

XML Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_OUTPUT SYSTEM "<qualys_base_url>/api/2.0/fo/asset/hos
t/dtd/list/output.dtd">
<HOST_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2023-05-10T12:20:39Z</DATETIME>
        <HOST_LIST>
            <HOST>
                <ID>2801679</ID>
                <IP>10.21.31.41</IP>
                <TRURISK_SCORE>514</TRURISK_SCORE>
                <ASSET_CRITICALITY_SCORE>3</ASSET_CRITICALITY_SCORE>
                <TRURISK_SCORE_FACTORS>

<TRURISK_SCORE_FORMULA>3 * {(1.0*95*(38^0.01))+(0.6*72*(107^0.01))+(0.4*4
8*(500^0.01))+(0.2*33*(1091^0.01))}</TRURISK_SCORE_FORMULA>
                    <VULN_COUNT qds_severity="1">0</VULN_COUNT>
                    <VULN_COUNT qds_severity="2">1091</VULN_COUNT>
                    <VULN_COUNT qds_severity="3">500</VULN_COUNT>
                    <VULN_COUNT qds_severity="4">107</VULN_COUNT>
                    <VULN_COUNT qds_severity="5">38</VULN_COUNT>
                </TRURISK_SCORE_FACTORS>
                <TRACKING_METHOD>IP</TRACKING_METHOD>
                <NETWORK_ID>0</NETWORK_ID>
                <DNS>
                    <![CDATA[10-21-31-41.bogus.tld]]>
                </DNS>
                <DNS_DATA>
                    <HOSTNAME>
                        <![CDATA[10-21-31-41]]>
                    </HOSTNAME>
                    <DOMAIN>
                        <![CDATA[bogus.tld]]>
                    </DOMAIN>
                    <FQDN>
                        <![CDATA[10-21-31-41.bogus.tld]]>
                    </FQDN>
```

```
                    </DNS_DATA>
                    <NETBIOS>
                        <![CDATA[SYS_10_21_31_41]]>
                    </NETBIOS>
                    <OS>
                        <![CDATA[Windows Server 2003 Service Pack 1]]>
                    </OS>
                    <FIRST_FOUND_DATE>2022-07-12T12:30:11Z</FIRST_FOUND_DATE>
                    <QG_HOSTID>
                        <![CDATA[c6656ff6-c4c3-40df-81b4-fffe361acf02]]>
                    </QG_HOSTID>
                    <FIRST_FOUND_DATE>2023-03-15T07:22:33Z</FIRST_FOUND_DATE>
                    <LAST_BOOT>2023-03-15T07:22:33Z</LAST_BOOT>
                  <SERIAL_NUMBER><![CDATA[hmhC53tK52oWfsv3]]></SERIAL_NUMBER>
                    <HARDWARE_UUID><![CDATA[08b829fb-ff42-8e41-a2ae-
1269ffc6872b]]></HARDWARE_UUID>
                    <LAST_ACTIVITY>2023-03-15T07:22:33Z</LAST_ACTIVITY>
                    <AGENT_STATUS><![CDATA[Inventory Scan
Complete]]></AGENT_STATUS>

<CLOUD_AGENT_RUNNING_ON><![CDATA[GCP]]></CLOUD_AGENT_RUNNING_ON>
                </HOST>
            </HOST_LIST>
        </RESPONSE>
</HOST_LIST_OUTPUT>
```

DTD Output:

We have updated the DTD for Host List Output to include the new elements (in bold).

DTD: <qualys_base_url>/api/2.0/fo/asset/host/dtd/list/output.dtd

```
<!-- QUALYS HOST_OUTPUT DTD FOR LIST ACTION-->
<!ELEMENT HOST_LIST_OUTPUT (REQUEST?,RESPONSE)>

<!ELEMENT REQUEST (DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?,
POST_DATA?)>
<!ELEMENT DATETIME (#PCDATA)>
<!ELEMENT USER_LOGIN (#PCDATA)>
<!ELEMENT RESOURCE (#PCDATA)>
<!ELEMENT PARAM_LIST (PARAM+)>
<!ELEMENT PARAM (KEY, VALUE)>
<!ELEMENT KEY (#PCDATA)>
<!ELEMENT VALUE (#PCDATA)>
<!-- if returned, POST_DATA will be urlencoded -->
<!ELEMENT POST_DATA (#PCDATA)>

<!ELEMENT RESPONSE (DATETIME, (HOST_LIST|ID_SET)?, WARNING?, GLOSSARY?)>
<!ELEMENT HOST_LIST (HOST+)>
```

```
<!ELEMENT HOST (ID, ASSET_ID?, IP?, IPV6?, TRURISK_SCORE?,
ASSET_CRITICALITY_SCORE?, TRURISK_SCORE_FACTORS?, TRACKING_METHOD?,
NETWORK_ID?,
                DNS?, DNS_DATA?, CLOUD_PROVIDER?, CLOUD_SERVICE?,
CLOUD_RESOURCE_ID?, EC2_INSTANCE_ID?, NETBIOS?, OS?, QG_HOSTID?,
LAST_BOOT?, SERIAL_NUMBER?, HARDWARE_UUID?, FIRST_FOUND_DATE?,
LAST_ACTIVITY?, AGENT_STATUS?, CLOUD_AGENT_RUNNING_ON?, TAGS?, METADATA?,
                CLOUD_PROVIDER_TAGS?, LAST_VULN_SCAN_DATETIME?,
LAST_VM_SCANNED_DATE?, LAST_VM_SCANNED_DURATION?,
              LAST_VM_AUTH_SCANNED_DATE?, LAST_VM_AUTH_SCANNED_DURATION?,
               LAST_COMPLIANCE_SCAN_DATETIME?, LAST_SCAP_SCAN_DATETIME?,
OWNER?, COMMENTS?, USER_DEF?, ASSET_GROUP_IDS?)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT ASSET_ID (#PCDATA)>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT IPV6 (#PCDATA)>
<!ELEMENT TRURISK_SCORE (#PCDATA)>
<!ELEMENT ASSET_CRITICALITY_SCORE (#PCDATA)>
<!ELEMENT TRURISK_SCORE_FACTORS (TRURISK_SCORE_FORMULA, VULN_COUNT*)>
<!ELEMENT TRURISK_SCORE_FORMULA (#PCDATA)>
<!ELEMENT VULN_COUNT (#PCDATA)>
...
<!ELEMENT QG_HOSTID (#PCDATA)>
<!ELEMENT LAST_BOOT (#PCDATA)>
<!ELEMENT SERIAL_NUMBER (#PCDATA)>
<!ELEMENT HARDWARE_UUID (#PCDATA)>
<!ELEMENT FIRST_FOUND_DATE (#PCDATA)>
<!ELEMENT LAST_ACTIVITY (#PCDATA)>
<!ELEMENT AGENT_STATUS (#PCDATA)>
<!ELEMENT CLOUD_AGENT_RUNNING_ON (#PCDATA)>
<!ELEMENT TAGS (TAG*)>
...
<!-- EOF -->
```

Download Saved Reports

APIs affected	/api/2.0/fo/report/?action=fetch
New or Updated API	Updated
DTD or XSD changes	Yes

With this release, all the ARS (Asset Risk Score) related parameters are renamed to replace ARS with TruRisk score in host-based scan reports, both XML and CSV formats.

Important: The old parameters with ARS will be retained for the next few releases. However, there will be a future update where these parameters will be removed with advance notification.

API Samples

Sample 1 - Download Host Based Scan Report in CSV Format

API Request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -d
"<qualys_base_url>/api/2.0/fo/report/?action=fetch&id=123457"
```

CSV Output:

```
"Sample Report","05/24/2023 at 18:17:24 (GMT-0800)"
"Qualys","919 E Hillsdale Blvd",,"Foster City","California","United
States of America","94404"
"Joe User","joe_user","Manager"
...
"IP","DNS","NetBIOS","QG Host ID","IP Interfaces","Tracking
Method","OS","IP Status","QID","Title","Vuln
Status","Type","Severity","Port","Protocol","FQDN","SSL","First
Detected","Last Detected","Times Detected","Date Last Fixed","First
Reopened","Last Reopened","Times Reopened","CVE ID","Vendor
Reference","Bugtraq
ID","Threat","Impact","Solution","Exploitability","Associated
Malware","Results","PCI Vuln","Ticket State","Instance","OS
CPE","Category","Associated Ags","Cloud Provider","Cloud Provider
Service","Cloud Service","Cloud Resource ID","Cloud Resource Type","Cloud
Account","Cloud Image ID","Cloud Resource Metadata","EC2 Instance
ID","Public Hostname","Image ID","VPC ID","Instance State","Private
Hostname","Instance Type","Account ID","Region Code","Subnet ID","Host
ID","Asset ID","QDS","TruRisk Score","ACS"
"10.20.30.40","10-20-30-40.bogus.tld",,,,"DNS",,"host scanned, found
vuln","100021","Microsoft Internet Explorer TABLE Status Bar URI
Obfuscation Weakness","New","Vuln","2",,,,,"05/24/2022
10:07:23","05/24/2022 10:07:23","1",,,,,"CVE-2005-
```

```
4679",,"11561","Microsoft Internet Explorer is reported prone to a URI
obfuscation weakness. The issue presents itself when a HREF tag contains
an additional HREF tag contained within a TABLE tag. It is reported that
hovering over the link of the second HREF tag will display the hostname
address of the first HREF tag in the status bar of Internet Explorer.
This weakness is reported to affect Internet Explorer 6, but other
versions may also be affected. Windows XP Service Pack 2 is not reported
to be vulnerable.","This issue may be leveraged by an attacker to display
false information in the status bar of an unsuspecting user, allowing an
attacker to present Web pages to users that seem to originate from a
trusted location. This may facilitate phishing style attacks. Other
attacks may also be possible.","This vulnerability is not exploitable with
Windows XP Service Pack 2. There are no solutions available at this time
for Windows 2000 or Windows XP Service Pack 1.",,,,"yes",,,,"Internet
Explorer",,,,,,,,,"[]",,,,,,,,,,,"2685870","14617851","28","104","4"
...
```

Sample 2 - Download Host Based Scan Report in XML Format

API Request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -d
"<qualys_base_url>/api/2.0/fo/report/?action=fetch&id=123456"
```

XML Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE ASSET_DATA_REPORT SYSTEM
"<qualys_base_url>/asset_data_report.dtd">
<ASSET_DATA_REPORT>
  <HEADER>
    <COMPANY>
      <![CDATA[ Qualys ]]>
    </COMPANY>
    <USERNAME>joe_user</USERNAME>
    <GENERATION_DATETIME>2022-05-24T15:30:56Z</GENERATION_DATETIME>
    <TEMPLATE>
      <![CDATA[ ARS_Report ]]>
    </TEMPLATE>
    <TARGET>
      <USER_IP_LIST>
        <RANGE>
          <START>10.20.30.40</START>
          <END>10.20.30.40</END>
        </RANGE>
      </USER_IP_LIST>
      <COMBINED_IP_LIST>
```

```
            <RANGE>
              <START>10.20.30.40</START>
              <END>10.20.30.40</END>
            </RANGE>
          </COMBINED_IP_LIST>
        </TARGET>
        <RISK_SCORE_SUMMARY>
          <TOTAL_VULNERABILITIES>5</TOTAL_VULNERABILITIES>
          <AVG_SECURITY_RISK>2.2</AVG_SECURITY_RISK>
          <BUSINESS_RISK>10/100</BUSINESS_RISK>
        </RISK_SCORE_SUMMARY>
      </HEADER>
      <RISK_SCORE_PER_HOST>
        <HOSTS>
          <IP_ADDRESS>10.20.30.40</IP_ADDRESS>
          <TOTAL_VULNERABILITIES>5</TOTAL_VULNERABILITIES>
          <SECURITY_RISK>2.2</SECURITY_RISK>
        </HOSTS>
      </RISK_SCORE_PER_HOST>
      <HOST_LIST>
        <HOST>
          <IP>10.20.30.40</IP>
          <TRACKING_METHOD>DNS</TRACKING_METHOD>
          <HOST_ID>2685870</HOST_ID>
          <ASSET_ID>14617851</ASSET_ID>
          <DNS>
            <![CDATA[ 10-20-30-40.bogus.tld ]]>
          </DNS>
          <TRURISK_SCORE>104</TRURISK_SCORE>
          <ACS>4</ACS>
          <VULN_INFO_LIST>
            <VULN_INFO>
              <QID id="qid_100027">100027</QID>
              <TYPE>Practice</TYPE>
              <SSL>false</SSL>
              <FIRST_FOUND>2022-05-24T04:37:23Z</FIRST_FOUND>
              <LAST_FOUND>2022-05-24T04:37:23Z</LAST_FOUND>
              <TIMES_FOUND>1</TIMES_FOUND>
              <VULN_STATUS>New</VULN_STATUS>
              <QDS>
                <![CDATA[ 32 ]]>
              </QDS>
            </VULN_INFO>
...
```

DTD Output:

We have updated the DTD for Asset Data Report Output to include the new elements (in bold).

DTD: <qualys_base_url>/asset_data_report.dtd

```
<!-- QUALYS ASSET DATA REPORT DTD -->
<!ELEMENT ASSET_DATA_REPORT (ERROR | (HEADER, RISK_SCORE_PER_HOST?,
HOST_LIST?, GLOSSARY?, NON_RUNNING_KERNELS?, APPENDICES?))>
<!ELEMENT ERROR (#PCDATA)*>
<!ATTLIST ERROR number CDATA #IMPLIED>
<!-- HEADER -->
<!ELEMENT HEADER (COMPANY, USERNAME?, GENERATION_DATETIME, TEMPLATE,
TARGET, RISK_SCORE_SUMMARY?)>

<!ELEMENT COMPANY (#PCDATA)>
<!ELEMENT USERNAME (#PCDATA)>
<!ELEMENT GENERATION_DATETIME (#PCDATA)>
<!ELEMENT TEMPLATE (#PCDATA)>
<!ELEMENT TARGET (USER_ASSET_GROUPS?, USER_IP_LIST?, COMBINED_IP_LIST?,
ASSET_TAG_LIST?)>

...

<!-- HOST_LIST -->

<!ELEMENT HOST_LIST (HOST+)>

<!ELEMENT HOST (ERROR | (IP?,IPV6?, TRACKING_METHOD, ASSET_TAGS?, HOST_ID,
ASSET_ID?,
                        DNS?, NETBIOS?, QG_HOSTID?, CLOUD_PROVIDER?,
CLOUD_PROVIDER_SERVICE?, CLOUD_SERVICE?, CLOUD_RESOURCE_TYPE?,
CLOUD_RESOURCE_ID?, CLOUD_ACCOUNT?, EC2_INSTANCE_ID?, CLOUD_IMAGE_ID?,
IP_INTERFACES?,EC2_INFO?, CLOUD_RESOURCE_METADATA?, AZURE_VM_INFO?,
OPERATING_SYSTEM?, OS_CPE?,
                        TRURISK_SCORE?, ACS?, ASSET_GROUPS?,
VULN_INFO_LIST?))>

<!ELEMENT IP (#PCDATA)>
...
<!ELEMENT TRURISK_SCORE (#PCDATA)>
<!ELEMENT ACS (#PCDATA)>
...
```

Enhanced Host Details

APIs affected	/api/2.0/fo/asset/host/?action=list
New or Updated API	Updated
DTD or XSD changes	Yes

With this release, to enhance the host asset data and improve asset visibility in integration systems, additional output parameters have been introduced in the response of the Host List API. These parameters mainly include the BIOS serial number and hardware UUID for each host detection. These parameters improve asset visibility in downstream integration systems and provide precise information about the asset's state.

Output Parameters

The following new parameters are added to the response:

Parameter	Description
LAST_ACTIVITY	(Agent Only) Shows the date and time when the host asset was last active.
LAST_BOOT	Shows the date and time when the host asset was last rebooted.
SERIAL_NUMBER	Shows the BIOS serial number of the asset.
HARDWARE_UUID	Shows the BIOS hardware UUID of the asset.
FIRST_FOUND_DATE	Shows the date and time when the asset was first listed or detected on Qualys platform.
AGENT_STATUS	(Agent Only) Shows the status or activity of the agent on the asset.
CLOUD_AGENT_RUNNING_ON	(Agent Only) Shows the name of the cloud on which the agent is deployed.

API Sample

Sample - List Host Assets

API Request:

```
curl --location --request GET
'<qualys_base_url>/api/2.0/fo/asset/host/?action=list&show_asset_id=1&host_metadata=all&details=All'
--header 'X-Requested-With: curl'
--header 'Authorization: <token>'
```

XML Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_OUTPUT SYSTEM
"<qualys_base_url>/api/2.0/fo/asset/host/dtd/list/output.dtd">
<HOST_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2023-04-25T03:52:05Z</DATETIME>
        <HOST_LIST>
            <HOST>
                <ID>32229</ID>
                <ASSET_ID>454545</ASSET_ID>
                <IP>10.14.28.129</IP>
                <TRACKING_METHOD>Cloud Agent</TRACKING_METHOD>
                <DNS>
                    <![CDATA[pt-w1122h2u]]>
                </DNS>
                <DNS_DATA>
                    <HOSTNAME>
                        <![CDATA[pt-w1122h2u]]>
                    </HOSTNAME>
                    <DOMAIN />
                    <FQDN />
                </DNS_DATA>
                <NETBIOS>
                    <![CDATA[PT-W1122H2U]]>
                </NETBIOS>
                <OS>
                    <![CDATA[Windows Microsoft Windows 11 Enterprise
10.0.22621 Build 22621]]>
                </OS>
                <QG_HOSTID>
                    <![CDATA[c6656ff6-c4c3-40df-81b4-fffe361acf02]]>
                </QG_HOSTID>
                <FIRST_FOUND_DATE>2023-03-15T07:22:33Z</FIRST_FOUND_DATE>
                <LAST_BOOT>2023-03-15T07:22:33Z</LAST_BOOT>
               <SERIAL_NUMBER><![CDATA[hmhC53tK52oWfsv3]]></SERIAL_NUMBER>
                <HARDWARE_UUID><![CDATA[08b829fb-ff42-8e41-a2ae-
1269ffc6872b]]></HARDWARE_UUID>
                <LAST_ACTIVITY>2023-03-15T07:22:33Z</LAST_ACTIVITY>
                <AGENT_STATUS><![CDATA[Inventory Scan
Complete]]></AGENT_STATUS>

<CLOUD_AGENT_RUNNING_ON><![CDATA[GCP]]></CLOUD_AGENT_RUNNING_ON>
            </HOST>
        </HOST_LIST>
    </RESPONSE>
</HOST_LIST_OUTPUT>
```

DTD Output:

We have updated the DTD for Host List Output to include the new elements (in bold).

DTD: <qualys_base_url>/api/2.0/fo/asset/host/dtd/list/output.dtd

```
<!-- QUALYS HOST_OUTPUT DTD FOR LIST ACTION-->
<!ELEMENT HOST_LIST_OUTPUT (REQUEST?,RESPONSE)>

<!ELEMENT REQUEST (DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?,
POST_DATA?)>
<!ELEMENT DATETIME (#PCDATA)>
<!ELEMENT USER_LOGIN (#PCDATA)>
<!ELEMENT RESOURCE (#PCDATA)>
<!ELEMENT PARAM_LIST (PARAM+)>
<!ELEMENT PARAM (KEY, VALUE)>
<!ELEMENT KEY (#PCDATA)>
<!ELEMENT VALUE (#PCDATA)>
<!-- if returned, POST_DATA will be urlencoded -->
<!ELEMENT POST_DATA (#PCDATA)>

<!ELEMENT RESPONSE (DATETIME, (HOST_LIST|ID_SET)?, WARNING?, GLOSSARY?)>
<!ELEMENT HOST_LIST (HOST+)>
<!ELEMENT HOST (ID, ASSET_ID?, IP?, IPV6?, TRURISK_SCORE?,
ASSET_CRITICALITY_SCORE?, TRURISK_SCORE_FACTORS?, TRACKING_METHOD?,
NETWORK_ID?,
                DNS?, DNS_DATA?, CLOUD_PROVIDER?, CLOUD_SERVICE?,
CLOUD_RESOURCE_ID?, EC2_INSTANCE_ID?, NETBIOS?, OS?, QG_HOSTID?,
LAST_BOOT?, SERIAL_NUMBER?, HARDWARE_UUID?, FIRST_FOUND_DATE?,
LAST_ACTIVITY?, AGENT_STATUS?, CLOUD_AGENT_RUNNING_ON?, TAGS?, METADATA?,
                CLOUD_PROVIDER_TAGS?, LAST_VULN_SCAN_DATETIME?,
LAST_VM_SCANNED_DATE?, LAST_VM_SCANNED_DURATION?,
              LAST_VM_AUTH_SCANNED_DATE?, LAST_VM_AUTH_SCANNED_DURATION?,
               LAST_COMPLIANCE_SCAN_DATETIME?, LAST_SCAP_SCAN_DATETIME?,
OWNER?, COMMENTS?, USER_DEF?, ASSET_GROUP_IDS?)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT ASSET_ID (#PCDATA)>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT IPV6 (#PCDATA)>
<!ELEMENT TRURISK_SCORE (#PCDATA)>
<!ELEMENT ASSET_CRITICALITY_SCORE (#PCDATA)>
<!ELEMENT TRURISK_SCORE_FACTORS (TRURISK_SCORE_FORMULA, VULN_COUNT*)>
<!ELEMENT TRURISK_SCORE_FORMULA (#PCDATA)>
<!ELEMENT VULN_COUNT (#PCDATA)>
...
<!ELEMENT QG_HOSTID (#PCDATA)>
<!ELEMENT LAST_BOOT (#PCDATA)>
<!ELEMENT SERIAL_NUMBER (#PCDATA)>
```

```
<!ELEMENT HARDWARE_UUID (#PCDATA)>
<!ELEMENT FIRST_FOUND_DATE (#PCDATA)>
<!ELEMENT LAST_ACTIVITY (#PCDATA)>
<!ELEMENT AGENT_STATUS (#PCDATA)>
<!ELEMENT CLOUD_AGENT_RUNNING_ON (#PCDATA)>
<!ELEMENT TAGS (TAG*)>
...
<!-- EOF -->
```

Introduced Unique IDs for Vulnerability Detections

APIs affected	/api/2.0/fo/asset/host/vm/detection/?action=list
New or Updated API	Updated
DTD or XSD changes	Yes

With this release, a new output parameter has been added to distinguish each vulnerability detection uniquely across different assets, ports, services, etc. This means that even if the same vulnerability is detected on multiple assets, each occurrence has a separate identifier to ensure individual identification.

Output Parameter

The following new parameter is added to the response:

Parameter	Description
UNIQUE_VULN_ID	Shows the unique ID of the vulnerability detection.

API Sample

Sample - List Host Detections

API Request:

```
curl --location --request GET
'<qualys_base_url>/api/2.0/fo/asset/host/vm/detection/?action=list&ips=10
.113.197.133&show_qds=1&show_asset_id=1&host_metadata=all'
--header 'X-Requested-With: curl'
--header 'Authorization: Basic <token>'
```

XML Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_VM_DETECTION_OUTPUT SYSTEM
"<qualys_base_url>/api/2.0/fo/asset/host/vm/detection/dtd/output.dtd">
<HOST_LIST_VM_DETECTION_OUTPUT>
    <RESPONSE>
        <DATETIME>2023-04-25T05:08:38Z</DATETIME>
        <HOST_LIST>
            <HOST>
                <ID>27124</ID>
                <ASSET_ID>81023</ASSET_ID>
                <IP>10.113.197.133</IP>
                <TRACKING_METHOD>IP</TRACKING_METHOD>
                <OS>
                    <![CDATA[Linux 2.6]]>
```

```
                </OS>
                <LAST_SCAN_DATETIME>2023-
0315T07:22:52Z</LAST_SCAN_DATETIME>
                <LAST_VM_SCANNED_DATE>2023-03-
15T07:21:27Z</LAST_VM_SCANNED_DATE>
                <LAST_VM_SCANNED_DURATION>1141</LAST_VM_SCANNED_DURATION>
                <DETECTION_LIST>
                    <DETECTION>
                        <UNIQUE_VULN_ID>52664</UNIQUE_VULN_ID>
                        <QID>11</QID>
                        <TYPE>Confirmed</TYPE>
                        <SEVERITY>2</SEVERITY>
                        <SSL>0</SSL>
                        <RESULTS>
                         <![CDATA[Name    Program Version Protocol    Port
                            portmap/rpcbind 100000  2-4 tcp 111
                            portmap/rpcbind 100000  2-4 udp 746]]>
                        </RESULTS>
                        <STATUS>New</STATUS>
                        <FIRST_FOUND_DATETIME>2023-03-
15T07:21:27Z</FIRST_FOUND_DATETIME>
                        <LAST_FOUND_DATETIME>2023-03-
15T07:21:27Z</LAST_FOUND_DATETIME>
                        <TIMES_FOUND>1</TIMES_FOUND>
                        <LAST_TEST_DATETIME>2023-03-
15T07:21:27Z</LAST_TEST_DATETIME>
                        <LAST_UPDATE_DATETIME>2023-03-
15T07:22:52Z</LAST_UPDATE_DATETIME>
                        <IS_IGNORED>0</IS_IGNORED>
                        <IS_DISABLED>0</IS_DISABLED>
                        <LAST_PROCESSED_DATETIME>2023-03-
15T07:22:52Z</LAST_PROCESSED_DATETIME>
                    </DETECTION>
                    <DETECTION>
                        <UNIQUE_VULN_ID>52655</DETECTION_ID>
                        <QID>13692</QID>
                        <TYPE>Potential</TYPE>
                        <SEVERITY>3</SEVERITY>
                        <PORT>8080</PORT>
                        <PROTOCOL>tcp</PROTOCOL>
                        <FQDN>
                            <![CDATA[10.113.197.133]]>
                        </FQDN>
                        <SSL>0</SSL>
                        <RESULTS>
                            <![CDATA[X-Jenkins: 2.121.2
                             Vulnerable Jenkins version found on port:
8080]]>
                        </RESULTS>
```

```
                        <STATUS>New</STATUS>
                        <FIRST_FOUND_DATETIME>2023-03-
15T07:21:27Z</FIRST_FOUND_DATETIME>
                        <LAST_FOUND_DATETIME>2023-03-
15T07:21:27Z</LAST_FOUND_DATETIME>
                        <TIMES_FOUND>1</TIMES_FOUND>
                        <LAST_TEST_DATETIME>2023-03-
15T07:21:27Z</LAST_TEST_DATETIME>
                        <LAST_UPDATE_DATETIME>2023-03-
15T07:22:52Z</LAST_UPDATE_DATETIME>
                        <IS_IGNORED>0</IS_IGNORED>
                        <IS_DISABLED>0</IS_DISABLED>
                        <LAST_PROCESSED_DATETIME>2023-03-
15T07:22:52Z</LAST_PROCESSED_DATETIME>
                    </DETECTION>
                </DETECTION_LIST>
            </HOST>
        </HOST_LIST>
    </RESPONSE>
</HOST_LIST_VM_DETECTION_OUTPUT>
```

DTD Output:

We have updated the DTD for Host List Detection output to include the new elements (in bold).

DTD: <qualys_base_url>/api/2.0/fo/asset/host/vm/detection/dtd/output.dtd

```
<!-- QUALYS HOST_LIST_VM_DETECTION_OUTPUT DTD -->
<!-- $Revision$ -->
<!ELEMENT HOST_LIST_VM_DETECTION_OUTPUT (REQUEST?,RESPONSE)>

<!ELEMENT REQUEST (DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?,
POST_DATA?)>
<!ELEMENT DATETIME (#PCDATA)>
<!ELEMENT USER_LOGIN (#PCDATA)>
<!ELEMENT RESOURCE (#PCDATA)>
<!ELEMENT PARAM_LIST (PARAM+)>
<!ELEMENT PARAM (KEY, VALUE)>
<!ELEMENT KEY (#PCDATA)>
<!ELEMENT VALUE (#PCDATA)>
...
<!ELEMENT DETECTION (UNIQUE_VULN_ID, QID, TYPE, SEVERITY?, PORT?,
PROTOCOL?, FQDN?, SSL?, INSTANCE?,
                     RESULTS?, STATUS?,
                    FIRST_FOUND_DATETIME?, LAST_FOUND_DATETIME?, SOURCE?,
QDS?, QDS_FACTORS?, TIMES_FOUND?,
                     LAST_TEST_DATETIME?,
                     LAST_UPDATE_DATETIME?,
                     LAST_FIXED_DATETIME?,
```

```
                    FIRST_REOPENED_DATETIME?, LAST_REOPENED_DATETIME?,
TIMES_REOPENED?,
                    SERVICE?, IS_IGNORED?, IS_DISABLED?,
AFFECT_RUNNING_KERNEL?, AFFECT_RUNNING_SERVICE?,
AFFECT_EXPLOITABLE_CONFIG?, LAST_PROCESSED_DATETIME?, ASSET_CVE?)>
<!ELEMENT UNIQUE_VULN_ID (#PCDATA)>
<!ELEMENT QID (#PCDATA)>
<!ELEMENT TYPE (#PCDATA)>
<!ELEMENT PORT (#PCDATA)>
<!ELEMENT PROTOCOL (#PCDATA)>
<!ELEMENT SSL (#PCDATA)>
...
<!-- EOF -->
```