Qualys Cloud Platform (VM, PC) v10.x

API Release Notes

Version 10.22.1

April 27, 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

Enabling TruRisk in Host-Based Scan Report Template

Supporting Kerberos Authentication in Unix Authentication Record

Fetching CPU, Memory, and Region Information of Scanners

Knowledgebase: Update in QIDs Modified Date in Change Log Section

Qualys 10.22.1 brings you many more improvements and updates! Learn more

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.

Enabling TruRisk in Host-Based Scan Report Template

APIs affected	/api/2.0/fo/report/template/scan/
New or Updated API	Updated
DTD or XSD changes	No

We have introduced a new parameter to enable TruRisk details in the host-based scan report template. This allows you to display the Qualys TruRisk details such as Asset Risk Score (ARS), Asset Criticality Score (ACS), and Qualys Detection Score (QDS) in host-based scan reports.

Note: This parameter is applicable only to the subscriptions that have Asset Risk Scoring (ARS) enabled.

Input Parameter

The following new input parameter is added:

Parameter	Mandatory?	Data type	Description
include_trueris k_details={0|1}	Optional	Boolean	Specify 0 to exclude and 1 to include TruRisk details in the report template. By default, the value is set to 1.

API Sample

Sample - Create a New Scan Report Template with TruRisk Details

API Request:

```
curl --location
'<qualys_base_url>/api/2.0/fo/report/template/scan/?action=create&report_
format=xml' \
--header 'Content-Type: text/xml' \
--header 'X-Requested-With: test' \
--header 'Authorization: Basic <token>' \
```

Request Body:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE REPORTTEMPLATE SYSTEM
"<qualys_base_url>/api/2.0/fo/report/template/scan/scanreporttemplate_inf
o.dtd">
<REPORTTEMPLATE>
   <SCANTEMPLATE>
      <TITLE>
         <INFO key="title"><![CDATA[TruRisk Host based API test]]></INFO>
```

```
      </TITLE>
      <TARGET>
         <INFO key="scan_selection"><![CDATA[HostBased]]></INFO>
         <INFO key="include_trending"><![CDATA[0]]></INFO>
         <INFO key="asset_groups"><![CDATA[ALL]]></INFO>
         <INFO key="network"><![CDATA[-100]]></INFO>
         <INFO key="ips" />
      </TARGET>
      <DISPLAY>
         <INFO key="graph_business_risk"><![CDATA[0]]></INFO>
         <INFO key="graph_vuln_over_time"><![CDATA[0]]></INFO>
         <INFO key="display_text_summary"><![CDATA[1]]></INFO>
         <INFO key="graph_status"><![CDATA[0]]></INFO>
         <INFO key="graph_potential_status"><![CDATA[0]]></INFO>
         <INFO key="sort_by"><![CDATA[host]]></INFO>
         <INFO key="cvss"><![CDATA[all]]></INFO>
         <INFO key="host_ag_details"><![CDATA[0]]></INFO>
         <INFO key="qualys_system_ids"><![CDATA[0]]></INFO>
         <INFO key="include_vuln_details_reopened"><![CDATA[1]]></INFO>
         <INFO key="cloud_provider_metadata"><![CDATA[0]]></INFO>
         <INFO key="include_truerisk_details"><![CDATA[1]]></INFO>
      </DISPLAY>
      <FILTER>
         <INFO key="selective_vulns"><![CDATA[complete]]></INFO>
         <INFO key="search_list_ids" />
         <INFO key="exclude_qid_option"><![CDATA[0]]></INFO>
         <INFO key="exclude_search_list_ids" />
         <INFO key="included_os"><![CDATA[ALL]]></INFO>
         <INFO key="status_new"><![CDATA[1]]></INFO>
         <INFO key="ig_active"><![CDATA[0]]></INFO>
         <INFO key="display_non_running_kernels"><![CDATA[0]]></INFO>
      </FILTER>
      <SERVICESPORTS>
         <INFO key="required_services" />
         <INFO key="unauthorized_services" />
         <INFO key="services_info" />
         <INFO key="required_ports" />
         <INFO key="unauthorized_ports" />
      </SERVICESPORTS>
      <USERACCESS>
         <INFO key="report_access_users" />
         <INFO key="global"><![CDATA[0]]></INFO>
      </USERACCESS>
   </SCANTEMPLATE>
</REPORTTEMPLATE>
```

XML Response:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
   <RESPONSE>
      <DATETIME>2023-03-15T10:56:44Z</DATETIME>
      <TEXT>Scan Report Template(s) Successfully Created.</TEXT>
      <ITEM_LIST>
         <ITEM>
            <KEY>ID</KEY>
            <VALUE>263435</VALUE>
         </ITEM>
      </ITEM_LIST>
   </RESPONSE>
</SIMPLE_RETURN>
```

Supporting Kerberos Authentication in Unix Authentication Record

APIs affected	/api/2.0/fo/auth/unix/
New or Updated API	Updated
DTD or XSD changes	Yes

With this release, Kerberos authentication is supported in Unix Authentication Record. You can create, edit, and list Unix Authentication Records with Kerberos credentials. This allows you to perform authenticated scans on Unix targets with Kerberos authentication enabled.

Input Parameters

Use the following parameters to configure Kerberos authentication in a Unix authentication record:

Parameter	Mandatory?	Data Type	Description
use_kerberos={0|1}	Optional	Boolean	Specify 1 to enable Kerberos authentication. By default, the value is set to 0.
realm_discovery={value}	Mandatory, if 'use_kerberos=1'	string	Specify the realm discovery method. The available values are manual, single, and DNS.
user_realm={value}	Mandatory, if 'use_kerberos=1'	string	Specify the realm name associated with a user's Kerberos principal.
service_realm={value}	Mandatory, if 'use_kerberos=1'	string	Specify the realm name associated with the Kerberos service or application that you are attempting to access. **Note:** This parameter is valid only if the "realm_discovery" parameter is set to "manual".
service_kdc={value}	Optional	string	Specify the Kerberos server that is responsible for issuing and validating service tickets. **Note:** This parameter is valid only if the "realm_discovery" parameter is set to "manual".
user_kdc={value}	Optional	string	Specify the Kerberos server that is responsible for authenticating users and issuing ticket granting tickets (TGTs) for a particular realm.

Parameter	Mandatory?	Data Type	Description
krb5_password ={value}	Mandatory, if 'use_kerberos= 1'	string	Enter the password to authenticate to the Kerberos Key Distribution Center (KDC).
krb5_login_type ={value}	Optional	string	Specify the type of login used to authenticate to the Kerberos Key Distribution Center (KDC). The available values are "basic" and "vault".
krb5_<vault parameters>={v alue}	Mandatory, if krb5_login_type =vault	string	If krb5_login_type is 'vault', then all vault parameter fields must be added with the prefix 'krb5_' For example, krb5_vault_type, krb5_vault_id, etc. The vault-specific parameters depend on the vault type you have selected. See the "Vault Definition" section in the API user guide.

API Samples

Sample 1 - Create a Unix Auth Record with Kerberos

.API Request:

```
curl --location --request POST
'<qualys_base_url>/api/2.0/fo/auth/unix/?username=root&action=create&ips=
10.0.0.1&title=unix krbs
api&use_kerberos=1&realm_discovery=manual&user_realm=realm.com&service_re
alm=abc.com&service_kdc=kdc&user_kdc=kerbs&krb5_password=123aa&krb5_login
_type=basic' \
--header 'X-Requested-With: portal' \
--header 'Authorization: Basic <token>' \
--data-raw ''
```

XML Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"<qualys_base_url>/api/2.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2023-02-09T06:54:59Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Created</TEXT>
                <ID_SET>
```

```
                    <ID>214500</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

DTD Output:

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

DTD: <qualys_base_url>/api/2.0/fo/auth/unix/auth_list_output.dtd

```
<!-- QUALYS AUTH_UNIX_LIST_OUTPUT DTD -->
        <!ELEMENT AUTH_UNIX_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, (AUTH_UNIX_LIST|ID_SET)?,
WARNING_LIST?, GLOSSARY?)>
        <!ELEMENT AUTH_UNIX_LIST (AUTH_UNIX+)>
        <!ELEMENT AUTH_UNIX (ID, TITLE, USERNAME, SKIP_PASSWORD?,
CLEARTEXT_PASSWORD?, TARGET_TYPE?, KERBEROS_AUTHENTICATION?,
REALM_DISCOVERY?, USER_REALM?, USER_KDC?, SERVICE_REALM?, SERVICE_KDC?,
KERBEROS_LOGIN_INFO?, (ROOT_TOOL?|ROOT_TOOL_INFO_LIST?),
((RSA_PRIVATE_KEY?, DSA_PRIVATE_KEY?)|PRIVATE_KEY_CERTIFICATE_LIST?),
PORT?, IP_SET?, IPV6_SET?, TAGS?, LOGIN_TYPE?, DIGITAL_VAULT?,
NETWORK_ID?, CREATED, LAST_MODIFIED, COMMENTS?, USE_AGENTLESS_TRACKING?,
AGENTLESS_TRACKING_PATH?, QUALYS_SHELL?)>
        <!ELEMENT ID (#PCDATA)>
        <!ELEMENT TITLE (#PCDATA)>
        <!ELEMENT USERNAME (#PCDATA)>
        <!ELEMENT SKIP_PASSWORD (#PCDATA)>
        <!ELEMENT CLEARTEXT_PASSWORD (#PCDATA)>
        <!ELEMENT TARGET_TYPE (#PCDATA)>
        <!ELEMENT KERBEROS_AUTHENTICATION (#PCDATA)>
        <!ELEMENT REALM_DISCOVERY (#PCDATA)>
        <!ELEMENT USER_REALM (#PCDATA)>
        <!ELEMENT USER_KDC (#PCDATA)>
        <!ELEMENT SERVICE_REALM (#PCDATA)>
```

```
<!ELEMENT SERVICE_KDC (#PCDATA)>
<!ELEMENT KERBEROS_LOGIN_INFO (DIGITAL_VAULT?)>
<!ATTLIST KERBEROS_LOGIN_INFO type (basic|vault) "basic">
<!ELEMENT ROOT_TOOL (#PCDATA)>
<!ELEMENT ROOT_TOOL_INFO_LIST (ROOT_TOOL_INFO)*>
<!ELEMENT RSA_PRIVATE_KEY EMPTY>
<!ELEMENT DSA_PRIVATE_KEY EMPTY>
<!ELEMENT PRIVATE_KEY_CERTIFICATE_LIST (PRIVATE_KEY_CERTIFICATE)*>
<!ELEMENT PORT (#PCDATA)>
...
<!-- EOF -->
```

Sample 2 - List Unix Auth Records with Kerberos Parameters

API Request:

```
curl --location --request POST
'<qualys_base_url>/api/2.0/fo/auth/unix/?action=list' \
--header 'X-Requested-With: portal' \
--header 'Authorization: Basic <token>' \
--data-raw ''
```

XML Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_UNIX_LIST_OUTPUT SYSTEM
"<qualys_base_url>/api/2.0/fo/auth/unix/dtd/auth_list_output.dtd">
<AUTH_UNIX_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2023-02-13T04:08:26Z</DATETIME>
        <AUTH_UNIX_LIST>
            <AUTH_UNIX>
                <ID>214497</ID>
                <TITLE>
                    <![CDATA[krbs]]>
                </TITLE>
                <USERNAME>
                    <![CDATA[root]]>
                </USERNAME>
                <SKIP_PASSWORD>0</SKIP_PASSWORD>
                <CLEARTEXT_PASSWORD>0</CLEARTEXT_PASSWORD>
                <TARGET_TYPE>
                    <![CDATA[Auto (default)]]>
                </TARGET_TYPE>
                <KERBEROS_AUTHENTICATION>1</KERBEROS_AUTHENTICATION>
                <REALM_DISCOVERY>
                    <![CDATA[manual]]>
                </REALM_DISCOVERY>
```

```
            <USER_REALM>
                <![CDATA[jsm.com]]>
            </USER_REALM>
            <USER_KDC>
                <![CDATA[kerbs.jsm.com]]>
            </USER_KDC>
            <SERVICE_REALM>
                <![CDATA[kerbs.jsm.com]]>
            </SERVICE_REALM>
            <SERVICE_KDC>
                <![CDATA[krb]]>
            </SERVICE_KDC>
            <IP_SET>
                <IP>0.0.0.0</IP>
            </IP_SET>
            <NETWORK_ID>0</NETWORK_ID>
            <CREATED>
                <DATETIME>2023-02-06T09:48:20Z</DATETIME>
                <BY>test_pq4</BY>
            </CREATED>
            <LAST_MODIFIED>
                <DATETIME>2023-02-06T12:30:33Z</DATETIME>
            </LAST_MODIFIED>
        </AUTH_UNIX>
        <AUTH_UNIX>
            <ID>214498</ID>
            <TITLE>
                <![CDATA[k1]]>
            </TITLE>
            <USERNAME>
                <![CDATA[root]]>
            </USERNAME>
            <SKIP_PASSWORD>0</SKIP_PASSWORD>
            <CLEARTEXT_PASSWORD>0</CLEARTEXT_PASSWORD>
            <TARGET_TYPE>
                <![CDATA[Auto (default)]]>
            </TARGET_TYPE>
            <KERBEROS_AUTHENTICATION>1</KERBEROS_AUTHENTICATION>
            <REALM_DISCOVERY>
                <![CDATA[manual]]>
            </REALM_DISCOVERY>
            <USER_REALM>
                <![CDATA[fwwqw]]>
            </USER_REALM>
            <USER_KDC>
                <![CDATA[user]]>
            </USER_KDC>
            <SERVICE_REALM>
                <![CDATA[s1sdd]]>
```

```
                    </SERVICE_REALM>
                    <SERVICE_KDC>
                        <![CDATA[]]>
                    </SERVICE_KDC>
                    <KERBEROS_LOGIN_INFO type="vault">
                        <DIGITAL_VAULT>
                            <DIGITAL_VAULT_ID>
                                <![CDATA[55014]]>
                            </DIGITAL_VAULT_ID>
                            <DIGITAL_VAULT_TYPE>
                                <![CDATA[Quest Vault]]>
                            </DIGITAL_VAULT_TYPE>
                            <DIGITAL_VAULT_TITLE>
                                <![CDATA[quest]]>
                            </DIGITAL_VAULT_TITLE>
                            <VAULT_SYSTEM_NAME>
                                <![CDATA[fhk]]>
                            </VAULT_SYSTEM_NAME>
                        </DIGITAL_VAULT>
                    </KERBEROS_LOGIN_INFO>
                    <IP_SET>
                        <IP>0.0.0.0</IP>
                    </IP_SET>
                    <NETWORK_ID>0</NETWORK_ID>
                    <CREATED>
                        <DATETIME>2023-02-06T12:54:00Z</DATETIME>
                        <BY>test_pq4</BY>
                    </CREATED>
                    <LAST_MODIFIED>
                        <DATETIME>2023-02-08T10:45:46Z</DATETIME>
                    </LAST_MODIFIED>
                </AUTH_UNIX>
            </AUTH_UNIX_LIST>
        </RESPONSE>
    </AUTH_UNIX_LIST_OUTPUT>
```

Fetching CPU, Memory, and Region Information of Scanners

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

With this release, you can retrieve the CPU, memory, and region information for a scanner appliance. This information helps you know the configuration and capacity of your scanner appliance and ensure the appliance is operating at its optimal level.

Note: To enable this feature for your subscription, contact your Technical Account Manager.

API Sample

Sample - CPU, Memory, and Region Information in Response

API Request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -d
"action=list&echo_request=1&output_mode=full"
"<qualys_base_url>/api/2.0/fo/appliance/"
```

XML Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE APPLIANCE_LIST_OUTPUT SYSTEM
"<qualys_base_url>/api/2.0/fo/appliance/appliance_list_output.dtd">
<APPLIANCE_LIST_OUTPUT>
    <REQUEST>
        <DATETIME>2023-03-27T08:24:13Z</DATETIME>
        <USER_LOGIN>vmsp_tc</USER_LOGIN>
        <RESOURCE><qualys_base_url>/api/2.0/fo/appliance/</RESOURCE>
        <PARAM_LIST>
          ...
        </PARAM_LIST>
    </REQUEST>
    <RESPONSE>
        <DATETIME>2023-03-27T08:24:13Z</DATETIME>
        <APPLIANCE_LIST>
            <APPLIANCE>
                <ID>23094</ID>
                <UUID>2e60caa5-027f-f87c-8364-fdd131923f98</UUID>
                ...
                <VLANS>
                    <SETTING>Disabled</SETTING>
                </VLANS>
                <STATIC_ROUTES />
```

```
                    <ML_LATEST>12.1.67-1</ML_LATEST>
                    <ML_VERSION updated="no">12.13.38-1</ML_VERSION>
                    <VULNSIGS_LATEST>2.5.730-2</VULNSIGS_LATEST>
                    ...
                    <MAX_CAPACITY_UNITS></MAX_CAPACITY_UNITS>
                    <CPU_INFO>Intel(R) Xeon(R) CPU E5-2699 v3 @
2.30GHz</CPU_INFO>
                    <MEMORY_INFO>2,070,484 MB</MEMORY_INFO>
                    <REGION_INFO></REGION_INFO>
                </APPLIANCE>
            </APPLIANCE_LIST>
        </RESPONSE>
</APPLIANCE_LIST_OUTPUT>
```

DTD Output:

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

DTD: <qualys_base_url>/api/2.0/fo/appliance/appliance_list_output.dtd

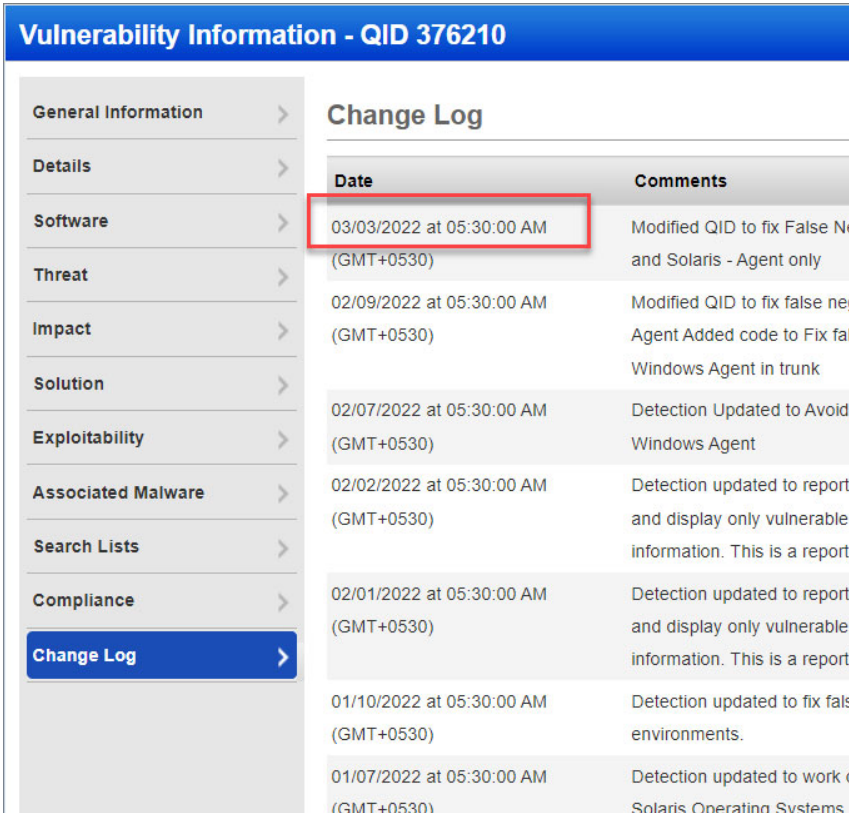
```
<!-- QUALYS APPLIANCE_LIST_OUTPUT DTD -->
<!ELEMENT APPLIANCE_LIST_OUTPUT (REQUEST?,RESPONSE)>

    <!ELEMENT REQUEST (DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?,
POST_DATA?)>
        <!ELEMENT DATETIME (#PCDATA)>
        ...
        <!ELEMENT APPLIANCE_LIST (APPLIANCE+)>
            <!ELEMENT APPLIANCE (ID, UUID, NAME, NETWORK_ID?,
SOFTWARE_VERSION, RUNNING_SLICES_COUNT, RUNNING_SCAN_COUNT, STATUS,
POOL_OF_SCANNERS?, CMD_ONLY_START?, MODEL_NUMBER?, TYPE?, SERIAL_NUMBER?,
..., RUNNING_SCANS?, MAX_CAPACITY_UNITS?, CPU_INFO?, MEMORY_INFO?,
REGION_INFO? )>
                <!ELEMENT ID (#PCDATA)>
                <!ELEMENT UUID (#PCDATA)>
                <!ELEMENT NAME (#PCDATA)>
                ...
                <!ELEMENT VLANS (SETTING, VLAN*)>
                    <!ELEMENT VLAN (ID, NAME, IP_ADDRESS?, NETMASK?,
IPV6_ADDRESS?, IPV6_SLAAC?)>
                        <!ELEMENT IPV6_SLAAC EMPTY>
                <!ELEMENT STATIC_ROUTES (ROUTE*)>
                  <!ELEMENT ROUTE (NAME, IP_ADDRESS?, NETMASK?, GATEWAY?,
IPV6_ADDRESS?, IPV6_NETWORK?, IPV6_GATEWAY?)>
                        <!ELEMENT IPV6_NETWORK (#PCDATA)>
                        <!ELEMENT IPV6_GATEWAY (#PCDATA)>
              ...
                <!ELEMENT COMMENTS (#PCDATA)>
                <!ELEMENT RUNNING_SCANS (SCAN+)>
```

```
                <!ELEMENT SCAN (ID, TITLE, REF, TYPE, SCAN_DATE)>
                    <!ELEMENT TITLE (#PCDATA)>
                    <!ELEMENT REF (#PCDATA)>
                    <!ELEMENT TYPE (#PCDATA)>
                    <!ELEMENT SCAN_DATE (#PCDATA)>
            <!ELEMENT MAX_CAPACITY_UNITS (#PCDATA)>
            <!ELEMENT CPU_INFO (#PCDATA)>
            <!ELEMENT MEMORY_INFO (#PCDATA)>
            <!ELEMENT REGION_INFO (#PCDATA)>
<!ELEMENT LICENSE_INFO (QVSA_LICENSES_COUNT, QVSA_LICENSES_USED)>
    <!ELEMENT QVSA_LICENSES_COUNT (#PCDATA)>
    <!ELEMENT QVSA_LICENSES_USED (#PCDATA)>
```

Knowlegebase: Update in QIDs Modified Date in Change Log Section

We have started publishing the QID change logs for 13 fields from June 2021. We also track the change dates in two date fields “KB modified date” and “RTI modified date”. The "service modified date" is using QID "insert date" and "modified date" instead of “KB modified date” and “RTI modified date”. We do not update QID "modified date" for all the 13 fields we are tracking as part of the change log.

Example: QID 376210, the service modified date is 05/30/2022 but the change log date shows the QID is modified on 03/03/2022



To avoid the date discrepancy which is observed in the "service modified date" and "change log" date, we will update the QID modified date for 13 fields that we are tracking as part of change log. With this release, you will not see the mismatch between change log date and service modified date.

There are 45+k QIDs in the back log which will get "service modified date" changes applicable. The oldest date that the “service modified date” will get updated to is "07-02-2018 00:00:00". Customers are required to start the sync from 07-02-2018 00:00:00

Use "/api/2.0/fo/knowledge_base/vuln/?action=list" API and input parameter “last_modified_by_service_after={date}” to reflect all the changes.

Below is the list of fields present in Change Log that will now be updated with "service modified date".

- Title

- Category

- Severity
- PCI Flag
- Authentication
- Remote flag
- CVE
- CVSS V2 Base Score
- CVSS V2 Temporal Score
- CVSS V3.1 Base Score
- CVSS V3.1 Temporal Score
- Exploits
- RTIs

Note: The change log for these fields & few more fields will be tracked in the upcoming release, which is planned for the end of March or early April of this year.

Issue Addressed

We have fixed an issue where a delay was faced for an API call which returns data with greater than 1000 records.