Qualys Cloud Platform (VM, PC) v10.x

API Release Notes

Version 10.24

September 11, 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

Cisco APIC 4.x Authentication Record

DNS BIND Authentication Record

PKCS8 Private Key Format Support for Unix Authentication Records

PKCS8 Private Key Format Support for Network SSH Authentication Records

Partial SSL/TLS Auditing

Filter Vulnerabilities Based on their Type

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.

Cisco APIC 4.x Authentication Record

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

This release introduces a new Cisco APIC authentication record API, which is available for the PC/SCA modules. Users can create/update Cisco APIC authentication records.

Input Parameters

The following new input parameters are added to the Cisco APIC authentication record.

Parameter	Required/ Optional	Data Type	Description
action	Required	String	Specify to list, create, update, delete, authentication records.
ids	Required	Integer	Specify a single or comma separated valid Cisco APIC type authentication record ID(s).
title	Required	Alpha-Numeric	Specify the title for the authentication record.
ips	Required	Integer	Specify the IP address(es) the server will log into using the record's credentials. Multiple entries are comma separated.
username	Required	String	Specify username for authentication login.
password	Required	String	Specify password for authentication login.
port	Required	Integer	Specify port number required on Cisco APIC devices.
ssl_verify	Optional	Integer	SSL verification is skipped by default. Set to 1 if you want to verify the server's certificate is valid and trusted.
Require Certificate	Optional	Alpha-Numeric	It contains two textfields, certificate and privatekey.
Vault Parameter			**Note:** The vault parameters are supported on the following vault types (Secret server Vault, Quest Vault, Hashicorp Vault, CyberArk AIM Vault, CyberArk PIM Vault, and AzureKey Vault).

Parameter	Required/ Optional	Data Type	Description
vault_type	Required	String	Specify if create, and login_type=vault. (private key only supports "Cyber-Ark AIM" and "BeyondTrust PBPS", whereas passphrase does not support "BeyondTrust PBPS").
vault_id	Required	Integer	Specify if create, and login_type=vault. The ID of the vault to be used to retrieve the password for login.
file	Required	String	Specify to create, if vault_type= "Cyber-Ark AIM" or "Cyber-ARK PIM Suite".
folder	Required	String	Specify to create, if vault_type="Cyber-Ark AIM" or "Cyber-ARK PIM Suite.
secret_name	Required	String	Specify to create, if vault_type="Thycotic Secret Server".
system_name	Required	String	Specify if yes(Quest) / no(BeyondTrust PBPS) (create, and vault_type="Quest Vault" or "BeyondTrust PBPS").
account_name	Required	String	Specify to create, if vault_type="BeyondTrust PBPS".

API Sample

Sample - List Cisco APIC auth records API

API Request:

```
curl -u "<token>" -H "X-Requested-With: curl" -d "action=list"
"http://qualys_base_url/api/2.0/fo/auth/cisco_apic/"
```

XML Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_CISCO_APIC_LIST_OUTPUT SYSTEM
"https://qualys_base_url/api/2.0/fo/auth/cisco_apic/auth_cisco_apic_list_
output.dtd">
<AUTH_CISCO_APIC_LIST_OUTPUT>
  <RESPONSE>
    <AUTH_CISCO_APIC_LIST>
      <AUTH_CISCO_APIC>
        <ID>7850382</ID>
        <TITLE><![CDATA[user 1]]></TITLE>
        <USERNAME><![CDATA[user 1]]></USERNAME>
        <PORT>444</PORT>
```

```
          <WINDOWS_DOMAIN><![CDATA[aaaa]]></WINDOWS_DOMAIN>
          <SSL_VERIFY><![CDATA[1]]></SSL_VERIFY>
          <IP_SET>
            <IP>3.3.3.3</IP>
          </IP_SET>
          <REQUIRE_CERT><![CDATA[1]]></REQUIRE_CERT>
          <DOMAIN><![CDATA[aaaa]]></DOMAIN>
          <PORT><![CDATA[444]]></PORT>
          <SSL_VERIFY_WITH_HOST><![CDATA[1]]></SSL_VERIFY_WITH_HOST>
          <LOGIN_TYPE><![CDATA[basic]]></LOGIN_TYPE>
          <CREATED>
            <BY>vt_sm1</BY>
          </CREATED>
        </AUTH_CISCO_APIC>
      </AUTH_CISCO_APIC_LIST>
    </RESPONSE>
</AUTH_CISCO_APIC_LIST_OUTPUT>
```

DTD Output:

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

```
<!-- QUALYS AUTH_RECORDS_OUTPUT DTD -->
<!ELEMENT AUTH_RECORDS_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_RECORDS?, WARNING_LIST?)>

<!ELEMENT AUTH_RECORDS (AUTH_UNIX_IDS?, AUTH_WINDOWS_IDS?,
AUTH_ORACLE_IDS?, AUTH_ORACLE_LISTENER_IDS?, AUTH_SNMP_IDS?,
AUTH_MS_SQL_IDS?, AUTH_IBM_DB2_IDS?, AUTH_VMWARE_IDS?, AUTH_MS_IIS_IDS?,
AUTH_APACHE_IDS?, AUTH_IBM_WEBSPHERE_IDS?, AUTH_HTTP_IDS?,
AUTH_SYBASE_IDS?, AUTH_MYSQL_IDS?, AUTH_TOMCAT_IDS?,
AUTH_ORACLE_WEBLOGIC_IDS?, AUTH_DOCKER_IDS?, AUTH_POSTGRESQL_IDS?,
AUTH_MONGODB_IDS?, AUTH_PALO_ALTO_FIREWALL_IDS?, AUTH_VCENTER_IDS?,
AUTH_JBOSS_IDS?, AUTH_MARIADB_IDS?, AUTH_INFORMIXDB_IDS?,
AUTH_MS_EXCHANGE_IDS?, AUTH_ORACLE_HTTP_SERVER_IDS?, AUTH_GREENPLUM_IDS?,
```

```
AUTH_MICROSOFT_SHAREPOINT_IDS?, AUTH_KUBERNETES_IDS?,
AUTH_SAPIQ_IDS?,AUTH_SAP_HANA_IDS?, AUTH_NEO4J_IDS?,
AUTH_AZURE_MS_SQL_IDS?, AUTH_NETWORK_SSH_IDS?, AUTH_NGINX_IDS?,
AUTH_INFOBLOX_IDS?, AUTH_CISCO_APIC_IDS?)>

<!ELEMENT AUTH_UNIX_IDS (ID_SET)>
<!ELEMENT AUTH_WINDOWS_IDS (ID_SET)>
<!ELEMENT AUTH_ORACLE_IDS (ID_SET)>
<!ELEMENT AUTH_ORACLE_LISTENER_IDS (ID_SET)>
<!ELEMENT AUTH_SNMP_IDS (ID_SET)>
<!ELEMENT AUTH_MS_SQL_IDS (ID_SET)>
<!ELEMENT AUTH_IBM_DB2_IDS (ID_SET)>
<!ELEMENT AUTH_VMWARE_IDS (ID_SET)>
<!ELEMENT AUTH_MS_IIS_IDS (ID_SET)>
<!ELEMENT AUTH_APACHE_IDS (ID_SET)>
<!ELEMENT AUTH_IBM_WEBSPHERE_IDS (ID_SET)>
<!ELEMENT AUTH_HTTP_IDS (ID_SET)>
<!ELEMENT AUTH_SYBASE_IDS (ID_SET)>
<!ELEMENT AUTH_MYSQL_IDS (ID_SET)>
<!ELEMENT AUTH_TOMCAT_IDS (ID_SET)>
<!ELEMENT AUTH_ORACLE_WEBLOGIC_IDS (ID_SET)>
<!ELEMENT AUTH_DOCKER_IDS (ID_SET)>
<!ELEMENT AUTH_POSTGRESQL_IDS (ID_SET)>
<!ELEMENT AUTH_MONGODB_IDS (ID_SET)>
<!ELEMENT AUTH_PALO_ALTO_FIREWALL_IDS (ID_SET)>
<!ELEMENT AUTH_VCENTER_IDS (ID_SET)>
<!ELEMENT AUTH_JBOSS_IDS (ID_SET)>
<!ELEMENT AUTH_MARIADB_IDS (ID_SET)>
<!ELEMENT AUTH_INFORMIXDB_IDS (ID_SET)>
<!ELEMENT AUTH_MS_EXCHANGE_IDS (ID_SET)>
<!ELEMENT AUTH_ORACLE_HTTP_SERVER_IDS (ID_SET)>
<!ELEMENT AUTH_GREENPLUM_IDS (ID_SET)>
<!ELEMENT AUTH_MICROSOFT_SHAREPOINT_IDS (ID_SET)>
<!ELEMENT AUTH_KUBERNETES_IDS (ID_SET)>
<!ELEMENT AUTH_SAPIQ_IDS (ID_SET)>
<!ELEMENT AUTH_SAP_HANA_IDS (ID_SET)>
<!ELEMENT AUTH_NEO4J_IDS (ID_SET)>
<!ELEMENT AUTH_AZURE_MS_SQL_IDS (ID_SET)>
<!ELEMENT AUTH_NETWORK_SSH_IDS (ID_SET)>
<!ELEMENT AUTH_NGINX_IDS (ID_SET)>
<!ELEMENT AUTH_INFOBLOX_IDS (ID_SET)>
<!ELEMENT AUTH_CISCO_APIC_IDS (ID_SET)>

<!ELEMENT WARNING_LIST (WARNING+)>
<!ELEMENT WARNING (CODE?, TEXT, URL?, ID_SET?)>
<!ELEMENT CODE (#PCDATA)>
<!ELEMENT TEXT (#PCDATA)>
<!ELEMENT URL (#PCDATA)>
```

```
<!ELEMENT ID_SET (ID|ID_RANGE)+>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT ID_RANGE (#PCDATA)>

<!-- EOF -->
```

Sample - Create Cisco APIC auth records Request API

API Request:

```
curl -u "<token>" -H "X-Requested-With: curl" -d
"action=create&ips=3.3.3.3&title=testciscoapic&username=admin&password=ab
c123&port=443" "http://qualys_base_url/api/2.0/fo/auth/cisco_apic/"
```

XML Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualys_base_url/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2023-08-09T11:03:04Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>7850988</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample - Update Cisco APIC auth records Request API

API Request:

```
curl -u "<token>" -H "X-Requested-With: curl" -d
"action=update&ids=7850382&title=testciscoapic"
"http://qualys_base_url/api/2.0/fo/auth/cisco_apic/"
```

XML Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualys_base_url/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
```

```
    <DATETIME>2023-08-09T10:48:33Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Updated</TEXT>
        <ID_SET>
          <ID>7850382</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

DTD Output:

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

```
<!-- QUALYS AUTH_CISCO_APIC_LIST_OUTPUT DTD -->

<!ELEMENT AUTH_CISCO_APIC_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_CISCO_APIC_LIST|ID_SET)?,
WARNING_LIST?, GLOSSARY?)>
<!ELEMENT AUTH_CISCO_APIC_LIST (AUTH_CISCO_APIC+)>

<!ELEMENT AUTH_CISCO_APIC (ID,
TITLE,USERNAME,SSL_VERIFY?,HOSTS?,REQUIRE_CERT?,CERTIFICATE?,PRIVATE_KEY?
,IP_SET?,PORT?,LOGIN_TYPE?,DIGITAL_VAULT?,NETWORK_ID?,CREATED,LAST_MODIFI
ED,COMMENTS?)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT USERNAME (#PCDATA)>
<!ELEMENT SSL_VERIFY (#PCDATA)>
<!ELEMENT IP_SET (IP|IP_RANGE)+>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT IP_RANGE (#PCDATA)>
<!ELEMENT PORT (#PCDATA)>
```

```
<!ELEMENT REQUIRE_CERT (#PCDATA)>
<!ELEMENT HOSTS (#PCDATA)>
<!ELEMENT CERTIFICATE (#PCDATA)>
<!ELEMENTPRIVATE_KEY (#PCDATA)>
<!ELEMENT LOGIN_TYPE (#PCDATA)>
<!ELEMENT DIGITAL_VAULT (DIGITAL_VAULT_ID, DIGITAL_VAULT_TYPE,
DIGITAL_VAULT_TITLE, VAULT_USERNAME?, VAULT_FOLDER?, VAULT_FILE?,
VAULT_SECRET_NAME?, VAULT_SYSTEM_NAME?, VAULT_NS_TYPE?, VAULT_NS_NAME?,
VAULT_SECRET_KV_PATH?, VAULT_SECRET_KV_NAME?, VAULT_SECRET_KV_KEY?,
VAULT_SERVICE_TYPE?)>
<!ELEMENT DIGITAL_VAULT_ID (#PCDATA)>
<!ELEMENT DIGITAL_VAULT_TYPE (#PCDATA)>
<!ELEMENT DIGITAL_VAULT_TITLE (#PCDATA)>
<!ELEMENT VAULT_USERNAME (#PCDATA)>
<!ELEMENT VAULT_FOLDER (#PCDATA)>
<!ELEMENT VAULT_FILE (#PCDATA)>
<!ELEMENT VAULT_SECRET_NAME (#PCDATA)>
<!ELEMENT VAULT_SYSTEM_NAME (#PCDATA)>
<!ELEMENT VAULT_NS_TYPE (#PCDATA)>
<!ELEMENT VAULT_NS_NAME (#PCDATA)>
<!ELEMENT VAULT_SECRET_KV_PATH (#PCDATA)>
<!ELEMENT VAULT_SECRET_KV_NAME (#PCDATA)>
<!ELEMENT VAULT_SECRET_KV_KEY (#PCDATA)>
<!ELEMENT VAULT_SERVICE_TYPE (#PCDATA)>

<!ELEMENT NETWORK_ID (#PCDATA)>

<!ELEMENT CREATED (DATETIME, BY)>
<!ELEMENT BY (#PCDATA)>
<!ELEMENT LAST_MODIFIED (DATETIME)>
<!ELEMENT COMMENTS (#PCDATA)>

<!ELEMENT WARNING_LIST (WARNING+)>
<!ELEMENT WARNING (CODE?, TEXT, URL?, ID_SET?)>
<!ELEMENT CODE (#PCDATA)>
<!ELEMENT TEXT (#PCDATA)>
<!ELEMENT URL (#PCDATA)>
<!ELEMENT ID_SET (ID|ID_RANGE)+>
<!ELEMENT ID_RANGE (#PCDATA)>

<!ELEMENT GLOSSARY (USER_LIST?)>
<!ELEMENT USER_LIST (USER+)>
<!ELEMENT USER (USER_LOGIN, FIRST_NAME, LAST_NAME)>
<!ELEMENT FIRST_NAME (#PCDATA)>
<!ELEMENT LAST_NAME (#PCDATA)>

<!-- EOF -->
```

DNS BIND Authentication Record

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

This release introduces a new BIND authentication record API, which is available for the PC/SCA modules. Users can create/update BIND authentication records.

Input Parameters

The following new input parameters are added to the BIND authentication record.

Parameter	Required/ Optional	Data Type	Description
action	Required	String	Specify to list, create, update, delete, authentication records.
ids	Required	Integer	Specify a single or comma separated valid DNS BIND type authentication record ID(s).
title	Required	Alpha-Numeric	Specify the title for the authentication record.
ips	Required	Integer	Specify the IP address(es) the server will log into using the record's credentials. Multiple entries are comma separated.
unix_bin_path	Required	Path	Specify absolute path of the DNS BIND Base64 encoded binary file location. Base64 encoded binary file path. Example- "/usr/sbin/named".
unix_conf_path	Required	Path	Specify absolute path of the DNS BIND Base64 encoded configuration file path. Example- "/etc/named.conf".
base_directory	Optional	Path	Specify Base64 encoded base directory. In BIND configuration file, if an include file is relative path, it is relative to this base_dir. Optional field, if not present, it will be derived from conf_path. Example- If conf_path is /etc/named.conf and if base_dir is not specified, then base_dir is set to "/etc". It must be absolute path if specified.

Parameter	Required/ Optional	Data Type	Description
chroot_directory	Optional	Path	Specify Base64 encoded chroot directory. Optional field, only needed if BIND runs in a self contained environment. If present, must be absolute path and it will be prefixed to all other 3 paths. Example- If chroot_dir is "/var/bind" and if bin_path is "/usr/sbin/named", then the final bin_path will be "/var/bind/usr/sbin/named".

API Sample

Sample - List DNS BIND auth records API

API Request:

```
curl" -d "action=list" "http://qualys_base_url/api/2.0/fo/auth/bind/"
```

XML Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_BIND_LIST_OUTPUT SYSTEM
"https://qualys_base_url/api/2.0/fo/auth/bind/auth_bind_list_output.dtd">
<AUTH_BIND_LIST_OUTPUT>
    <AUTH_BIND_LIST>
      <AUTH_BIND>
        <ID>7882778</ID>
        <TITLE><![CDATA[user_1]]></TITLE>
        <IP_SET>
          <IP>40.40.40.6</IP>
        </IP_SET>
        <UNIX_BIN_PATH><![CDATA[/usr/bin/bind]]></UNIX_BIN_PATH>
        <UNIX_CONF_PATH><![CDATA[/etc/bind/bind.conf]]></UNIX_CONF_PATH>
        <BASE_DIRECTORY><![CDATA[/etc/bind]]></BASE_DIRECTORY>
        <CHROOT_DIRECTORY><![CDATA[/etc/bind]]></CHROOT_DIRECTORY>
        <CREATED>
          <DATETIME>2023-08-14T16:15:57Z</DATETIME>
          <BY>vt_sm1</BY>
        </CREATED>
        <LAST_MODIFIED>
          <DATETIME>2023-08-14T16:15:57Z</DATETIME>
        </LAST_MODIFIED>
      </AUTH_BIND>
    </AUTH_BIND_LIST>
  </RESPONSE>
</AUTH_BIND_LIST_OUTPUT>
```

Sample - Create DNS BIND auth records Request API

API Request:

```
curl" -d
"action=create&ips=40.40.40.6&title=user_1bind2c&unix_bin_path=/etc&unix_
conf_path=/etc/bind" "http://qualys_base_url:48443/api/2.0/fo/auth/bind/"
```

XML Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualys_base_url/api/2.0/batch_return.dtd">
<BATCH_RETURN>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>7882779</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample - Update DNS BIND auth records Request API

API Request:

```
curl" -d "action=update&ids=7882778&title=testbind"
"http://qualys_base_url:48443/api/2.0/fo/auth/bind/"
```

XML Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualys_base_url/api/2.0/batch_return.dtd">
<BATCH_RETURN>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Updated</TEXT>
        <ID_SET>
          <ID>7882778</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

DTD Output:

Auth Record list output DTD

```
<!-- QUALYS AUTH_RECORDS_OUTPUT DTD -->
<!ELEMENT AUTH_RECORDS_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_RECORDS?, WARNING_LIST?)>

<!ELEMENT AUTH_RECORDS (AUTH_UNIX_IDS?, AUTH_WINDOWS_IDS?,
AUTH_ORACLE_IDS?, AUTH_ORACLE_LISTENER_IDS?, AUTH_SNMP_IDS?,
AUTH_MS_SQL_IDS?, AUTH_IBM_DB2_IDS?, AUTH_VMWARE_IDS?, AUTH_MS_IIS_IDS?,
AUTH_APACHE_IDS?, AUTH_IBM_WEBSPHERE_IDS?, AUTH_HTTP_IDS?,
AUTH_SYBASE_IDS?, AUTH_MYSQL_IDS?, AUTH_TOMCAT_IDS?,
AUTH_ORACLE_WEBLOGIC_IDS?, AUTH_DOCKER_IDS?, AUTH_POSTGRESQL_IDS?,
AUTH_MONGODB_IDS?, AUTH_PALO_ALTO_FIREWALL_IDS?, AUTH_VCENTER_IDS?,
AUTH_JBOSS_IDS?, AUTH_MARIADB_IDS?, AUTH_INFORMIXDB_IDS?,
AUTH_MS_EXCHANGE_IDS?, AUTH_ORACLE_HTTP_SERVER_IDS?, AUTH_GREENPLUM_IDS?,
AUTH_MICROSOFT_SHAREPOINT_IDS?, AUTH_KUBERNETES_IDS?,
AUTH_SAPIQ_IDS?,AUTH_SAP_HANA_IDS?, AUTH_NEO4J_IDS?,
AUTH_AZURE_MS_SQL_IDS?, AUTH_NETWORK_SSH_IDS?, AUTH_NGINX_IDS?,
AUTH_INFOBLOX_IDS?, AUTH_BIND_IDS?)>

<!ELEMENT AUTH_UNIX_IDS (ID_SET)>
<!ELEMENT AUTH_WINDOWS_IDS (ID_SET)>
<!ELEMENT AUTH_ORACLE_IDS (ID_SET)>
<!ELEMENT AUTH_ORACLE_LISTENER_IDS (ID_SET)>
<!ELEMENT AUTH_SNMP_IDS (ID_SET)>
<!ELEMENT AUTH_MS_SQL_IDS (ID_SET)>
<!ELEMENT AUTH_IBM_DB2_IDS (ID_SET)>
<!ELEMENT AUTH_VMWARE_IDS (ID_SET)>
<!ELEMENT AUTH_MS_IIS_IDS (ID_SET)>
<!ELEMENT AUTH_APACHE_IDS (ID_SET)>
<!ELEMENT AUTH_IBM_WEBSPHERE_IDS (ID_SET)>
<!ELEMENT AUTH_HTTP_IDS (ID_SET)>
<!ELEMENT AUTH_SYBASE_IDS (ID_SET)>
```

```
<!ELEMENT AUTH_MYSQL_IDS (ID_SET)>
<!ELEMENT AUTH_TOMCAT_IDS (ID_SET)>
<!ELEMENT AUTH_ORACLE_WEBLOGIC_IDS (ID_SET)>
<!ELEMENT AUTH_DOCKER_IDS (ID_SET)>
<!ELEMENT AUTH_POSTGRESQL_IDS (ID_SET)>
<!ELEMENT AUTH_MONGODB_IDS (ID_SET)>
<!ELEMENT AUTH_PALO_ALTO_FIREWALL_IDS (ID_SET)>
<!ELEMENT AUTH_VCENTER_IDS (ID_SET)>
<!ELEMENT AUTH_JBOSS_IDS (ID_SET)>
<!ELEMENT AUTH_MARIADB_IDS (ID_SET)>
<!ELEMENT AUTH_INFORMIXDB_IDS (ID_SET)>
<!ELEMENT AUTH_MS_EXCHANGE_IDS (ID_SET)>
<!ELEMENT AUTH_ORACLE_HTTP_SERVER_IDS (ID_SET)>
<!ELEMENT AUTH_GREENPLUM_IDS (ID_SET)>
<!ELEMENT AUTH_MICROSOFT_SHAREPOINT_IDS (ID_SET)>
<!ELEMENT AUTH_KUBERNETES_IDS (ID_SET)>
<!ELEMENT AUTH_SAPIQ_IDS (ID_SET)>
<!ELEMENT AUTH_SAP_HANA_IDS (ID_SET)>
<!ELEMENT AUTH_NEO4J_IDS (ID_SET)>
<!ELEMENT AUTH_AZURE_MS_SQL_IDS (ID_SET)>
<!ELEMENT AUTH_NETWORK_SSH_IDS (ID_SET)>
<!ELEMENT AUTH_NGINX_IDS (ID_SET)>
<!ELEMENT AUTH_INFOBLOX_IDS (ID_SET)>
<!ELEMENT AUTH_BIND_IDS (ID_SET)>

<!ELEMENT WARNING_LIST (WARNING+)>
<!ELEMENT WARNING (CODE?, TEXT, URL?, ID_SET?)>
<!ELEMENT CODE (#PCDATA)>
<!ELEMENT TEXT (#PCDATA)>
<!ELEMENT URL (#PCDATA)>

<!ELEMENT ID_SET (ID|ID_RANGE)+>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT ID_RANGE (#PCDATA)>

<!-- EOF -->
```

DTD: <qualys_base_url>/aapi/2.0/fo/auth/auth_bind_list_output.dtd

Auth Infoblox list output DTD

```
<!-- QUALYS AUTH_BIND_LIST_OUTPUT DTD -->
<!ELEMENT AUTH_BIND_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_BIND_LIST|ID_SET)?, WARNING_LIST?,
GLOSSARY?)>
<!ELEMENT AUTH_BIND_LIST (AUTH_BIND+)>

<!ELEMENT AUTH_BIND (ID,
TITLE,IP_SET?,UNIX_BIN_PATH?,UNIX_CONF_PATH?,BASE_DIRECTORY?,CHROOT_DIREC
TORY?,NETWORK_ID?,CREATED,LAST_MODIFIED,COMMENTS?)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT IP_SET (IP|IP_RANGE)+>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT IP_RANGE (#PCDATA)>
<!ELEMENT UNIX_BIN_PATH (#PCDATA)>
<!ELEMENT UNIX_CONF_PATH (#PCDATA)>
<!ELEMENT BASE_DIRECTORY (#PCDATA)>
<!ELEMENT CHROOT_DIRECTORY (#PCDATA)>
<!ELEMENT NETWORK_ID (#PCDATA)>

<!ELEMENT CREATED (DATETIME, BY)>
<!ELEMENT BY (#PCDATA)>
<!ELEMENT LAST_MODIFIED (DATETIME)>
<!ELEMENT COMMENTS (#PCDATA)>

<!ELEMENT WARNING_LIST (WARNING+)>
<!ELEMENT WARNING (CODE?, TEXT, URL?, ID_SET?)>
<!ELEMENT CODE (#PCDATA)>
<!ELEMENT TEXT (#PCDATA)>
<!ELEMENT URL (#PCDATA)>
<!ELEMENT ID_SET (ID|ID_RANGE)+>
<!ELEMENT ID_RANGE (#PCDATA)>

<!ELEMENT GLOSSARY (USER_LIST?)>
<!ELEMENT USER_LIST (USER+)>
<!ELEMENT USER (USER_LOGIN, FIRST_NAME, LAST_NAME)>
<!ELEMENT FIRST_NAME (#PCDATA)>
<!ELEMENT LAST_NAME (#PCDATA)>

<!-- EOF -->
```

PKCS8 Private Key Format Support for Unix Authentication Records

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

With this release, you can now create/edit authentication records in FIPS mode with private keys in PKCS8 format. The PKCS8 private key format enables to resolve validation errors while creating or editing authentication records with private keys in FIPS mode.

API Sample

API Request:

```
curl -k -u agms_nb:Qatemp123# -s -S -H 'X-Requested-With:curl demo2' -d
"action=list" "<qualys_base_url>/api/2.0/fo/auth/unix/"
```

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>2023-09-05T08:48:12Z</DATETIME>
    <AUTH_UNIX_LIST>
      <AUTH_UNIX>
        <ID>321277</ID>
        <TITLE><![CDATA[API_v2_END_TO_END_agms_nb_UNIX]]></TITLE>
        <USERNAME><![CDATA[root]]></USERNAME>
        <SKIP_PASSWORD>0</SKIP_PASSWORD>
        <CLEARTEXT_PASSWORD>0</CLEARTEXT_PASSWORD>
        <IP_SET>
          <IP>10.10.10.10</IP>
        </IP_SET>
        <NETWORK_ID>0</NETWORK_ID>
        <CREATED>
          <DATETIME>2019-10-15T08:48:06Z</DATETIME>
          <BY>agms_nb</BY>
        </CREATED>
        <LAST_MODIFIED>
          <DATETIME>2019-10-15T08:48:06Z</DATETIME>
        </LAST_MODIFIED>
        <QUALYS_SHELL>
```

```
            <ENABLED>0</ENABLED>
          </QUALYS_SHELL>
        </AUTH_UNIX>
 ...
<AUTH_UNIX>
        <ID>3382464</ID>
        <TITLE><![CDATA[unn]]></TITLE>
        <USERNAME><![CDATA[admin]]></USERNAME>
        <SKIP_PASSWORD>0</SKIP_PASSWORD>
        <CLEARTEXT_PASSWORD>0</CLEARTEXT_PASSWORD>
        <TARGET_TYPE><![CDATA[Auto (default)]]></TARGET_TYPE>
        <PRIVATE_KEY_CERTIFICATE_LIST>
          <PRIVATE_KEY_CERTIFICATE>
            <ID>2257361</ID>
            <PRIVATE_KEY_INFO type="basic">
              <PRIVATE_KEY type="pkcs8" />
            </PRIVATE_KEY_INFO>
            <PASSPHRASE_INFO type="basic" />
          </PRIVATE_KEY_CERTIFICATE>
          <PRIVATE_KEY_CERTIFICATE>
            <ID>2257360</ID>
            <PRIVATE_KEY_INFO type="basic">
              <PRIVATE_KEY type="pkcs8" />
            </PRIVATE_KEY_INFO>
            <PASSPHRASE_INFO type="basic" />
          </PRIVATE_KEY_CERTIFICATE>
          <PRIVATE_KEY_CERTIFICATE>
            <ID>2255896</ID>
            <PRIVATE_KEY_INFO type="basic">
              <PRIVATE_KEY type="pkcs8" />
            </PRIVATE_KEY_INFO>
            <PASSPHRASE_INFO type="basic" />
          </PRIVATE_KEY_CERTIFICATE>
        </PRIVATE_KEY_CERTIFICATE_LIST> <IP_SET>
          <IP>1.9.0.8</IP>
        </IP_SET>
        <NETWORK_ID>0</NETWORK_ID>
        <CREATED>
          <DATETIME>2023-08-23T09:40:11Z</DATETIME>
          <BY>agms_nb</BY>
        </CREATED>
        <LAST_MODIFIED>
          <DATETIME>2023-08-24T10:04:07Z</DATETIME>
        </LAST_MODIFIED>
        <QUALYS_SHELL>
          <ENABLED>0</ENABLED>
        </QUALYS_SHELL>
      </AUTH_UNIX>
```

DTD Update

DTD Changes	Added pkcs8 type in private key type.

DTD Output:

```
<!-- QUALYS AUTH_UNIX_LIST_OUTPUT DTD -->
        <!-- $Revision$ -->
        <!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)>

        <!ELEMENT IP_SET (IP|IP_RANGE)+>
        <!ELEMENT IP (#PCDATA)>
        <!ELEMENT IP_RANGE (#PCDATA)>

        <!ELEMENT IPV6_SET (IPV6|IPV6_RANGE)+>
        <!ELEMENT IPV6 (#PCDATA)>
        <!ELEMENT IPV6_RANGE (#PCDATA)>

        <!ELEMENT TAGS (TAG_TYPE, TAGS_INCLUDE, TAGS_EXCLUDE?)>
        <!ELEMENT TAG_TYPE (#PCDATA)>
        <!ELEMENT TAGS_INCLUDE (SELECTOR, TAG+)>
        <!ELEMENT SELECTOR (#PCDATA)>
        <!ELEMENT TAG (ID, NAME)>
        <!ELEMENT NAME (#PCDATA)>
        <!ELEMENT TAGS_EXCLUDE (SELECTOR, TAG?)>

        <!ELEMENT LOGIN_TYPE (#PCDATA)>
        <!ELEMENT NETWORK_ID (#PCDATA)>
        <!ELEMENT CREATED (DATETIME, BY)>
        <!ELEMENT BY (#PCDATA)>
        <!ELEMENT LAST_MODIFIED (DATETIME)>
        <!ELEMENT COMMENTS (#PCDATA)>
        <!ELEMENT USE_AGENTLESS_TRACKING (#PCDATA)>
        <!ELEMENT AGENTLESS_TRACKING_PATH (#PCDATA)>
        <!ELEMENT QUALYS_SHELL (ENABLED, LOG_FACILITY?)>


        <!ELEMENT ROOT_TOOL_INFO (ID, ROOT_TOOL, PASSWORD_INFO?)>
        <!ELEMENT PASSWORD_INFO (DIGITAL_VAULT?)>
        <!ATTLIST PASSWORD_INFO type (basic|vault) "basic">


        <!-- Private key contents will never be rendered -->
        <!ELEMENT PRIVATE_KEY_CERTIFICATE (ID, PRIVATE_KEY_INFO,
PASSPHRASE_INFO, CERTIFICATE?)+>
        <!ELEMENT PRIVATE_KEY_INFO (PRIVATE_KEY|DIGITAL_VAULT)>
        <!ATTLIST PRIVATE_KEY_INFO type (basic|vault) "basic">
        <!-- Private key/Certificate contents will never be rendered -->
        <!ELEMENT PRIVATE_KEY EMPTY>
        <!ATTLIST PRIVATE_KEY type (rsa|dsa|ecdsa|ed25519|pkcs8)
```

```
#REQUIRED>

        <!ELEMENT PASSPHRASE_INFO (DIGITAL_VAULT?)>
        <!ATTLIST PASSPHRASE_INFO type (basic|vault) "basic">
        <!ELEMENT CERTIFICATE EMPTY>
        <!ATTLIST CERTIFICATE type (x.509|openssh) #REQUIRED>
        <!ELEMENT DIGITAL_VAULT (DIGITAL_VAULT_ID, DIGITAL_VAULT_TYPE,
DIGITAL_VAULT_TITLE, VAULT_USERNAME?, VAULT_FOLDER?, VAULT_FILE?,
VAULT_SECRET_NAME?, VAULT_SYSTEM_NAME?, VAULT_EP_NAME?, VAULT_EP_TYPE?,
VAULT_EP_CONT?, VAULT_NS_TYPE?, VAULT_NS_NAME?, VAULT_ACCOUNT_NAME?,
VAULT_AUTHORIZATION_NAME?, VAULT_TARGET_NAME?, VAULT_SECRET_KV_PATH?,
VAULT_SECRET_KV_NAME?, VAULT_SECRET_KV_KEY?, VAULT_DEVICE_NAME?,
VAULT_DEVICE_HOST?, VAULT_APP_NAME?, VAULT_SERVICE_TYPE?)>
        <!ELEMENT DIGITAL_VAULT_ID (#PCDATA)>
        <!ELEMENT DIGITAL_VAULT_TYPE (#PCDATA)>
        <!ELEMENT DIGITAL_VAULT_TITLE (#PCDATA)>
        <!ELEMENT VAULT_USERNAME (#PCDATA)>
        <!ELEMENT VAULT_FOLDER (#PCDATA)>
        <!ELEMENT VAULT_FILE (#PCDATA)>
        <!ELEMENT VAULT_SECRET_NAME (#PCDATA)>
        <!ELEMENT VAULT_SYSTEM_NAME (#PCDATA)>
        <!ELEMENT VAULT_EP_NAME (#PCDATA)>
        <!ELEMENT VAULT_EP_TYPE (#PCDATA)>
        <!ELEMENT VAULT_EP_CONT (#PCDATA)>
        <!ELEMENT VAULT_NS_TYPE (#PCDATA)>
        <!ELEMENT VAULT_NS_NAME (#PCDATA)>
        <!ELEMENT VAULT_ACCOUNT_NAME (#PCDATA)>
        <!ELEMENT VAULT_AUTHORIZATION_NAME (#PCDATA)>
        <!ELEMENT VAULT_TARGET_NAME (#PCDATA)>
        <!ELEMENT VAULT_SECRET_KV_PATH (#PCDATA)>
        <!ELEMENT VAULT_SECRET_KV_NAME (#PCDATA)>
        <!ELEMENT VAULT_SECRET_KV_KEY (#PCDATA)>
        <!ELEMENT VAULT_DEVICE_NAME (#PCDATA)>
        <!ELEMENT VAULT_DEVICE_HOST (#PCDATA)>
        <!ELEMENT VAULT_APP_NAME (#PCDATA)>
        <!ELEMENT VAULT_SERVICE_TYPE (#PCDATA)>
        <!ELEMENT ENABLED (#PCDATA)>
        <!ELEMENT LOG_FACILITY (#PCDATA)>

        <!ELEMENT WARNING_LIST (WARNING+)>
        <!ELEMENT WARNING (CODE?, TEXT, URL?, ID_SET?)>
        <!ELEMENT CODE (#PCDATA)>
        <!ELEMENT TEXT (#PCDATA)>
        <!ELEMENT URL (#PCDATA)>
        <!ELEMENT ID_SET (ID|ID_RANGE)+>
        <!ELEMENT ID_RANGE (#PCDATA)>

        <!ELEMENT GLOSSARY (USER_LIST?)>
        <!ELEMENT USER_LIST (USER+)>
```

```
<!ELEMENT USER (USER_LOGIN, FIRST_NAME, LAST_NAME)>
<!ELEMENT FIRST_NAME (#PCDATA)>
<!ELEMENT LAST_NAME (#PCDATA)>

<!-- EOF -->
```

PKCS8 Private Key Format Support for Network SSH Authentication Records

APIs affected	/api/2.0/fo/auth/network_ssh/
New or Updated API	Updated
DTD or XSD changes	YES

With this release, you can now create/edit authentication records in FIPS mode with private keys in PKCS8 format. The PKCS8 private key format enables to resolve validation errors while creating or editing authentication records with private keys in FIPS mode.

API Sample

API Request:

```
curl -k -u agms_nb:Qatemp123# -s -S -H 'X-Requested-With:curl demo2' -d
"action=list" "<qualys_base_url>/api/2.0/fo/auth/network_ssh/"
```

XML Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_NETWORK_SSH_LIST_OUTPUT SYSTEM
"<qualys_base_url>/api/2.0/fo/auth/network_ssh/dtd/auth_list_output.dtd">
<AUTH_NETWORK_SSH_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2023-09-05T08:44:22Z</DATETIME>
    <AUTH_NETWORK_SSH_LIST>
      <AUTH_NETWORK_SSH>
        <ID>3441133</ID>
        <TITLE><![CDATA[API_Unix_Auth_Unix_21]]></TITLE>
        <USERNAME><![CDATA[Qualys]]></USERNAME>
        <IP_SET>
          <IP>10.10.10.10</IP>
        </IP_SET>
        <CLEARTEXT_PASSWORD>0</CLEARTEXT_PASSWORD>
        <TARGET_TYPE><![CDATA[Auto (default)]]></TARGET_TYPE>
        <PRIVATE_KEY_CERTIFICATE_LIST>
          <PRIVATE_KEY_CERTIFICATE>
            <ID>2274448</ID>
            <PRIVATE_KEY_INFO type="basic">
              <PRIVATE_KEY type="pkcs8" />
            </PRIVATE_KEY_INFO>
            <PASSPHRASE_INFO type="basic" />
          </PRIVATE_KEY_CERTIFICATE>
```

```
          </PRIVATE_KEY_CERTIFICATE_LIST>
          <NETWORK_ID>0</NETWORK_ID>
          <CREATED>
            <DATETIME>2023-09-04T15:43:07Z</DATETIME>
            <BY>agms_nb</BY>
          </CREATED>
          <LAST_MODIFIED>
            <DATETIME>2023-09-04T15:43:07Z</DATETIME>
          </LAST_MODIFIED>
        </AUTH_NETWORK_SSH>
      </AUTH_NETWORK_SSH_LIST>
    </RESPONSE>
</AUTH_NETWORK_SSH_LIST_OUTPUT>
```

DTD Update

DTD Changes — Added pkcs8 type in private key type.

DTD Output

```
<!-- QUALYS NETWORK_SSH_LIST_OUTPUT DTD -->
        <!-- $Revision$ -->
        <!ELEMENT AUTH_NETWORK_SSH_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_NETWORK_SSH_LIST|ID_SET)?,
WARNING_LIST?, GLOSSARY?)>
        <!ELEMENT AUTH_NETWORK_SSH_LIST (AUTH_NETWORK_SSH+)>
        <!ELEMENT AUTH_NETWORK_SSH (ID, TITLE, USERNAME, PORT?, IP_SET?,
LOGIN_TYPE?, DIGITAL_VAULT?, CLEARTEXT_PASSWORD?, PASSWORD2_INFO?,
TARGET_TYPE?, ((RSA_PRIVATE_KEY?,
DSA_PRIVATE_KEY?)|PRIVATE_KEY_CERTIFICATE_LIST?), NETWORK_ID?, CREATED,
```

```
LAST_MODIFIED, COMMENTS?)>
        <!ELEMENT ID (#PCDATA)>
        <!ELEMENT TITLE (#PCDATA)>
        <!ELEMENT USERNAME (#PCDATA)>
        <!ELEMENT CLEARTEXT_PASSWORD (#PCDATA)>
        <!ELEMENT TARGET_TYPE (#PCDATA)>
        <!ELEMENT RSA_PRIVATE_KEY EMPTY>
        <!ELEMENT DSA_PRIVATE_KEY EMPTY>
       <!ELEMENT PRIVATE_KEY_CERTIFICATE_LIST (PRIVATE_KEY_CERTIFICATE)*>
        <!ELEMENT PORT (#PCDATA)>

        <!ELEMENT IP_SET (IP|IP_RANGE)+>
        <!ELEMENT IP (#PCDATA)>
        <!ELEMENT IP_RANGE (#PCDATA)>


        <!ELEMENT LOGIN_TYPE (#PCDATA)>
        <!ELEMENT PASSWORD2_INFO (DIGITAL_VAULT?)>
        <!ATTLIST PASSWORD2_INFO type (basic|vault) "basic">
        <!ELEMENT NETWORK_ID (#PCDATA)>
        <!ELEMENT CREATED (DATETIME, BY)>
        <!ELEMENT BY (#PCDATA)>
        <!ELEMENT LAST_MODIFIED (DATETIME)>
        <!ELEMENT COMMENTS (#PCDATA)>

        <!-- Private key contents will never be rendered -->
        <!ELEMENT PRIVATE_KEY_CERTIFICATE (ID, PRIVATE_KEY_INFO,
PASSPHRASE_INFO, CERTIFICATE?)+>
        <!ELEMENT PRIVATE_KEY_INFO (PRIVATE_KEY|DIGITAL_VAULT)>
        <!ATTLIST PRIVATE_KEY_INFO type (basic|vault) "basic">
        <!-- Private key/Certificate contents will never be rendered -->
        <!ELEMENT PRIVATE_KEY EMPTY>
        <!ATTLIST PRIVATE_KEY type (rsa|dsa|ecdsa|ed25519|pkcs8)
#REQUIRED>

        <!ELEMENT PASSPHRASE_INFO (DIGITAL_VAULT?)>
        <!ATTLIST PASSPHRASE_INFO type (basic|vault) "basic">

        <!ELEMENT CERTIFICATE EMPTY>
        <!ATTLIST CERTIFICATE type (x.509|openssh) #REQUIRED>
        <!ELEMENT DIGITAL_VAULT (DIGITAL_VAULT_ID, DIGITAL_VAULT_TYPE,
DIGITAL_VAULT_TITLE, VAULT_USERNAME?, VAULT_FOLDER?, VAULT_FILE?,
VAULT_SECRET_NAME?, VAULT_SYSTEM_NAME?, VAULT_EP_NAME?, VAULT_EP_TYPE?,
VAULT_EP_CONT?, VAULT_NS_TYPE?, VAULT_NS_NAME?, VAULT_ACCOUNT_NAME?,
VAULT_AUTHORIZATION_NAME?, VAULT_TARGET_NAME?, VAULT_SECRET_KV_PATH?,
VAULT_SECRET_KV_NAME?, VAULT_SECRET_KV_KEY?, VAULT_DEVICE_NAME?,
VAULT_DEVICE_HOST?, VAULT_APP_NAME?, VAULT_SERVICE_TYPE?)>
        <!ELEMENT DIGITAL_VAULT_ID (#PCDATA)>
        <!ELEMENT DIGITAL_VAULT_TYPE (#PCDATA)>
```

```
<!ELEMENT DIGITAL_VAULT_TITLE (#PCDATA)>
<!ELEMENT VAULT_USERNAME (#PCDATA)>
<!ELEMENT VAULT_FOLDER (#PCDATA)>
<!ELEMENT VAULT_FILE (#PCDATA)>
<!ELEMENT VAULT_SECRET_NAME (#PCDATA)>
<!ELEMENT VAULT_SYSTEM_NAME (#PCDATA)>
<!ELEMENT VAULT_EP_NAME (#PCDATA)>
<!ELEMENT VAULT_EP_TYPE (#PCDATA)>
<!ELEMENT VAULT_EP_CONT (#PCDATA)>
<!ELEMENT VAULT_NS_TYPE (#PCDATA)>
<!ELEMENT VAULT_NS_NAME (#PCDATA)>
<!ELEMENT VAULT_ACCOUNT_NAME (#PCDATA)>
<!ELEMENT VAULT_AUTHORIZATION_NAME (#PCDATA)>
<!ELEMENT VAULT_TARGET_NAME (#PCDATA)>
<!ELEMENT VAULT_SECRET_KV_PATH (#PCDATA)>
<!ELEMENT VAULT_SECRET_KV_NAME (#PCDATA)>
<!ELEMENT VAULT_SECRET_KV_KEY (#PCDATA)>
<!ELEMENT VAULT_DEVICE_NAME (#PCDATA)>
<!ELEMENT VAULT_DEVICE_HOST (#PCDATA)>
<!ELEMENT VAULT_APP_NAME (#PCDATA)>
<!ELEMENT VAULT_SERVICE_TYPE (#PCDATA)>


<!ELEMENT WARNING_LIST (WARNING+)>
<!ELEMENT WARNING (CODE?, TEXT, URL?, ID_SET?)>
<!ELEMENT CODE (#PCDATA)>
<!ELEMENT TEXT (#PCDATA)>
<!ELEMENT URL (#PCDATA)>
<!ELEMENT ID_SET (ID|ID_RANGE)+>
<!ELEMENT ID_RANGE (#PCDATA)>

<!ELEMENT GLOSSARY (USER_LIST?)>
<!ELEMENT USER_LIST (USER+)>
<!ELEMENT USER (USER_LOGIN, FIRST_NAME, LAST_NAME)>
<!ELEMENT FIRST_NAME (#PCDATA)>
<!ELEMENT LAST_NAME (#PCDATA)>

<!-- EOF -->
```

Partial SSL/TLS Auditing

APIs affected	/api/2.0/fo/subscription/option_profile/vm/?action=create /api/2.0/fo/subscription/option_profile/vm/?action=update /api/2.0/fo/subscription/option_profile/?action=export /api/2.0/fo/subscription/option_profile/?action=import
New or Updated API	Updated
DTD or XSD changes	YES

With this release, you can partially scan SSL/TLS endpoints with an incomplete handshake. An incomplete handshake occurs when SSL/TLS endpoints require client certificates to complete SSL/TLS handshake. Only a subset of QIDs is checked in this mode. Any QIDs that are typically reported as confirmed vulnerabilities are now reported as potential vulnerabilities.

Input Parameter

The following new parameter is added to the request. This is an optional parameter.

Parameter	Description
enable_partial_ssl_tls_auditing = {0|1}	Use to enable or disable the partial SSL/TLS auditing during scan execution. Specify 1 to enable partial SSL/TLS checks while executing the scan.

API Samples

Sample - Create VM Option Profile with SSL/TLS auditing enabled

API Request:

```
curl --location --request POST
'<qualys_base_url>/api/2.0/fo/subscription/option_profile/vm/?%20action=c
reate&title=VM_API_Option_profile_696969&scan_tcp_ports=none&scan_udp_por
ts=none&vulnerability_detection=complete&basic_information_gathering=none
&enable_partial_ssl_tls_auditing=1' \

--header 'Content-Type: application/x-www-form-urlencoded' \
--header 'X-Requested-With: curl demo2' \
--header 'Accept: */*' \
--header 'Content-Length: 0' \
--header 'Authorization: Basic <encoded username:password string>'
```

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>2023-08-31T10:05:16Z</DATETIME>
        <TEXT>Option profile successfully added.</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>2445054</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Update VM option profile with SSL/TLS auditing disabled

API Request:

```
ccurl --location --request POST
'<qualys_base_url>/api/2.0/fo/subscription/option_profile/vm/?enable_part
ial_ssl_tls_auditing=0&%20action=update&id=2437618&scan_tcp_ports=standar
d&scan_udp_ports=standard&vulnerability_detection=runtime' \

--header 'Content-Type: application/x-www-form-urlencoded' \
--header 'X-Requested-With: curl demo2' \
--header 'Accept: */*' \
--header 'Content-Length: 0' \
--header 'Authorization: Basic <encoded username:password string>'
```

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>2023-08-31T10:04:24Z</DATETIME>
        <TEXT>Option profile successfully updated.</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>2437618</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Option Profile Export

API Request:

```
curl --location
'<qualys_base_url>/api/2.0/fo/subscription/option_profile/?action=export&
option_profile_title=VM_API_Option_profile_01' \

--header 'Content-Type: application/x-www-form-urlencoded' \
--header 'X-Requested-With: curl demo2' \
--header 'Accept: */*' \
--header 'Content-Length: 0' \
--header 'Authorization: Basic <encoded username:password string>'
```

XML Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM
"<qualys_base_url>/api/2.0/fo/subscription/option_profile/option_profile_
info.dtd">
<OPTION_PROFILES>
    <OPTION_PROFILE>
        <BASIC_INFO>
            <ID>2445050</ID>
            <GROUP_NAME>
                <![CDATA[VM_API_Option_profile_01]]>
            </GROUP_NAME>
            <GROUP_TYPE>user</GROUP_TYPE>
            <USER_ID>
                <![CDATA[Automation Test (scan_at)]]>
            </USER_ID>
            <UNIT_ID>0</UNIT_ID>
            <SUBSCRIPTION_ID>590924</SUBSCRIPTION_ID>
            <IS_DEFAULT>0</IS_DEFAULT>
            <IS_GLOBAL>0</IS_GLOBAL>
            <IS_OFFLINE_SYNCABLE>0</IS_OFFLINE_SYNCABLE>
            <UPDATE_DATE>2023-08-31T09:34:28Z</UPDATE_DATE>
        </BASIC_INFO>
        <SCAN>
            <PORTS>
                <TCP_PORTS>
                    <TCP_PORTS_TYPE>none</TCP_PORTS_TYPE>
                    <THREE_WAY_HANDSHAKE>0</THREE_WAY_HANDSHAKE>
                </TCP_PORTS>
                <UDP_PORTS>
                    <UDP_PORTS_TYPE>none</UDP_PORTS_TYPE>
                </UDP_PORTS>
                <AUTHORITATIVE_OPTION>0</AUTHORITATIVE_OPTION>
            </PORTS>
            <SCAN_DEAD_HOSTS>0</SCAN_DEAD_HOSTS>
```

```
                <PURGE_OLD_HOST_OS_CHANGED>0</PURGE_OLD_HOST_OS_CHANGED>
                <PERFORMANCE>
                    <PARALLEL_SCALING>0</PARALLEL_SCALING>
                    <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
                    <HOSTS_TO_SCAN>
                        <EXTERNAL_SCANNERS>15</EXTERNAL_SCANNERS>
                        <SCANNER_APPLIANCES>30</SCANNER_APPLIANCES>
                    </HOSTS_TO_SCAN>
                    <PROCESSES_TO_RUN>
                        <TOTAL_PROCESSES>10</TOTAL_PROCESSES>
                        <HTTP_PROCESSES>10</HTTP_PROCESSES>
                    </PROCESSES_TO_RUN>
                    <PACKET_DELAY>Medium</PACKET_DELAY>

<PORT_SCANNING_AND_HOST_DISCOVERY>Normal</PORT_SCANNING_AND_HOST_DISCOVER
Y>
                    <HOST_CGI_CHECKS>0</HOST_CGI_CHECKS>
                    <MAX_TARGETS_PER_SLICE>0</MAX_TARGETS_PER_SLICE>

<CONF_SCAN_LIMITED_CONNECTIVITY>0</CONF_SCAN_LIMITED_CONNECTIVITY>
                    <SKIP_PRE_SCANNING>0</SKIP_PRE_SCANNING>
                </PERFORMANCE>
                <LOAD_BALANCER_DETECTION>0</LOAD_BALANCER_DETECTION>
                <VULNERABILITY_DETECTION>
                    <COMPLETE>
                        <![CDATA[complete]]>
                    </COMPLETE>
                    <DETECTION_INCLUDE>
                        <BASIC_HOST_INFO_CHECKS>0</BASIC_HOST_INFO_CHECKS>
                        <OVAL_CHECKS>0</OVAL_CHECKS>
                        <QRDI_CHECKS>0</QRDI_CHECKS>
                    </DETECTION_INCLUDE>
                </VULNERABILITY_DETECTION>
                <ADDL_CERT_DETECTION>0</ADDL_CERT_DETECTION>

<PERFORM_PARTIAL_SSL_TLS_AUDITING>1</PERFORM_PARTIAL_SSL_TLS_AUDITING>
            </SCAN>
            <MAP>
                <BASIC_INFO_GATHERING_ON>none</BASIC_INFO_GATHERING_ON>
                <MAP_OPTIONS>
                    <PERFORM_LIVE_HOST_SWEEP>0</PERFORM_LIVE_HOST_SWEEP>
                    <DISABLE_DNS_TRAFFIC>0</DISABLE_DNS_TRAFFIC>
                </MAP_OPTIONS>
                <MAP_PERFORMANCE>
                    <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
                    <MAP_PARALLEL>
                        <EXTERNAL_SCANNERS>6</EXTERNAL_SCANNERS>
                        <SCANNER_APPLIANCES>8</SCANNER_APPLIANCES>
                        <NETBLOCK_SIZE>16384 IPs</NETBLOCK_SIZE>
```

```
                    </MAP_PARALLEL>
                    <PACKET_DELAY>Minimum</PACKET_DELAY>
                </MAP_PERFORMANCE>
                <MAP_AUTHENTICATION>none</MAP_AUTHENTICATION>
            </MAP>
            <ADDITIONAL>
                <HOST_DISCOVERY>
                    <TCP_PORTS>
                        <STANDARD_SCAN>1</STANDARD_SCAN>
                    </TCP_PORTS>
                    <UDP_PORTS>
                        <STANDARD_SCAN>1</STANDARD_SCAN>
                    </UDP_PORTS>
                    <ICMP>1</ICMP>
                </HOST_DISCOVERY>
                <PACKET_OPTIONS>

<IGNORE_FIREWALL_GENERATED_TCP_RST>0</IGNORE_FIREWALL_GENERATED_TCP_RST>
                    <IGNORE_ALL_TCP_RST>0</IGNORE_ALL_TCP_RST>

<IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>0</IGNORE_FIREWALL_GENERATED_TCP_S
YN_ACK>

<NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>0</NOT_SEND_TCP_ACK_OR
_SYN_ACK_DURING_HOST_DISCOVERY>
                </PACKET_OPTIONS>
            </ADDITIONAL>
        </OPTION_PROFILE>
</OPTION_PROFILES>
```

Sample - Option Profile Import

API Request:

```
curl --location
'<qualys_base_url>/api/2.0/fo/subscription/option_profile/?action=import'
\

--header 'X-Requested-With: curl demo2' \
--header 'Accept: */*' \
--header 'Content-Type: text/xml' \
--header 'Authorization: Basic <encoded username:password string>' \
--data '<?xml version="1.0" encoding="UTF-8" ?>

<!DOCTYPE OPTION_PROFILES SYSTEM
"<qualys_base_url>/api/2.0/fo/subscription/option_profile/option_profile_
info.dtd">

<OPTION_PROFILES>
  <OPTION_PROFILE>
    <BASIC_INFO>
      <ID>1599154</ID>
      <GROUP_NAME><![CDATA[API_IMPORT_OP_1647433780]]></GROUP_NAME>
      <GROUP_TYPE>user</GROUP_TYPE>
      <USER_ID><![CDATA[Network Disabled (pv_nd)]]></USER_ID>
      <UNIT_ID>0</UNIT_ID>
      <SUBSCRIPTION_ID>915185</SUBSCRIPTION_ID>
      <IS_DEFAULT>0</IS_DEFAULT>
      <IS_GLOBAL>0</IS_GLOBAL>
      <IS_OFFLINE_SYNCABLE>0</IS_OFFLINE_SYNCABLE>
      <UPDATE_DATE>2019-03-19T09:13:26Z</UPDATE_DATE>
    </BASIC_INFO>
    <SCAN>
      <PORTS>
        <TCP_PORTS>
          <TCP_PORTS_TYPE>standard</TCP_PORTS_TYPE>
          <THREE_WAY_HANDSHAKE>0</THREE_WAY_HANDSHAKE>
        </TCP_PORTS>
        <UDP_PORTS>
          <UDP_PORTS_TYPE>standard</UDP_PORTS_TYPE>
        </UDP_PORTS>
        <AUTHORITATIVE_OPTION>0</AUTHORITATIVE_OPTION>
      </PORTS>
      <SCAN_DEAD_HOSTS>0</SCAN_DEAD_HOSTS>
      <PERFORMANCE>

        <PARALLEL_SCALING>0</PARALLEL_SCALING>
        <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
        <HOSTS_TO_SCAN>
          <EXTERNAL_SCANNERS>15</EXTERNAL_SCANNERS>
```

```
            <SCANNER_APPLIANCES>30</SCANNER_APPLIANCES>
          </HOSTS_TO_SCAN>
          <PROCESSES_TO_RUN>
            <TOTAL_PROCESSES>10</TOTAL_PROCESSES>
            <HTTP_PROCESSES>10</HTTP_PROCESSES>
          </PROCESSES_TO_RUN>
          <PACKET_DELAY>Medium</PACKET_DELAY>

<PORT_SCANNING_AND_HOST_DISCOVERY>Normal</PORT_SCANNING_AND_HOST_DISCOVER
Y>
      </PERFORMANCE>
      <LOAD_BALANCER_DETECTION>0</LOAD_BALANCER_DETECTION>
      <VULNERABILITY_DETECTION>
        <COMPLETE><![CDATA[complete]]></COMPLETE>
        <DETECTION_INCLUDE>
          <BASIC_HOST_INFO_CHECKS>0</BASIC_HOST_INFO_CHECKS>
          <OVAL_CHECKS>0</OVAL_CHECKS>
        </DETECTION_INCLUDE>
      </VULNERABILITY_DETECTION>
      <AUTHENTICATION><![CDATA[Windows,Unix,Oracle,Oracle
Listener,SNMP,VMware,DB2,HTTP,MySQL,MongoDB,Tomcat Server,Oracle Weblogic
Server,Palo Alto Networks Firewall,Jboss Server]]></AUTHENTICATION>

      <ADDL_CERT_DETECTION>0</ADDL_CERT_DETECTION>
      <TEST_AUTHENTICATION>1</TEST_AUTHENTICATION>
   <PERFORM_PARTIAL_SSL_TLS_AUDITING>1</PERFORM_PARTIAL_SSL_TLS_AUDITING>
    </SCAN>
    <MAP>
      <BASIC_INFO_GATHERING_ON>all</BASIC_INFO_GATHERING_ON>
      <TCP_PORTS>
        <TCP_PORTS_STANDARD_SCAN>1</TCP_PORTS_STANDARD_SCAN>
      </TCP_PORTS>
      <MAP_OPTIONS>
        <PERFORM_LIVE_HOST_SWEEP>1</PERFORM_LIVE_HOST_SWEEP>
        <DISABLE_DNS_TRAFFIC>0</DISABLE_DNS_TRAFFIC>
      </MAP_OPTIONS>
      <MAP_PERFORMANCE>
        <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
        <MAP_PARALLEL>
          <EXTERNAL_SCANNERS>6</EXTERNAL_SCANNERS>
          <SCANNER_APPLIANCES>8</SCANNER_APPLIANCES>
          <NETBLOCK_SIZE>16384 IPs</NETBLOCK_SIZE>
        </MAP_PARALLEL>
        <PACKET_DELAY>Minimum</PACKET_DELAY>

      </MAP_PERFORMANCE>
      <MAP_AUTHENTICATION>none</MAP_AUTHENTICATION>
    </MAP>
    <ADDITIONAL>
```

```
      <HOST_DISCOVERY>
        <TCP_PORTS>
          <STANDARD_SCAN>1</STANDARD_SCAN>
        </TCP_PORTS>
        <UDP_PORTS>
          <STANDARD_SCAN>1</STANDARD_SCAN>
        </UDP_PORTS>
        <ICMP>1</ICMP>
      </HOST_DISCOVERY>
      <PACKET_OPTIONS>
 <IGNORE_FIREWALL_GENERATED_TCP_RST>0</IGNORE_FIREWALL_GENERATED_TCP_RST>
        <IGNORE_ALL_TCP_RST>0</IGNORE_ALL_TCP_RST>
<IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>0</IGNORE_FIREWALL_GENERATED_TCP_S
YN_ACK>
<NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>0</NOT_SEND_TCP_ACK_OR
_SYN_ACK_DURING_HOST_DISCOVERY>
      </PACKET_OPTIONS>
    </ADDITIONAL>
  </OPTION_PROFILE>
</OPTION_PROFILES>
```

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>2023-08-31T10:08:47Z</DATETIME>
       <TEXT>Successfully imported Option profile for the subscription Id
590924</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>2445059</KEY>
                <VALUE>API_IMPORT_OP_1647433780</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

DTD Update

API affected	/api/2.0/fo/subscription/option_profile/?action=export /api/2.0/fo/subscription/option_profile/?action=import
DTD changes	Added a new DTD element, <PERFORM_PARTIAL_SSL_TLS_AUDITING>

DTD Output

Option Profile Import

```
<!-- QUALYS SIMPLE_RETURN DTD -->
<!-- $Revision$ -->
<!ELEMENT SIMPLE_RETURN (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 specified, POST_DATA will be urlencoded -->
<!ELEMENT POST_DATA (#PCDATA)>
<!ELEMENT RESPONSE (DATETIME, CODE?, TEXT, ITEM_LIST?)>
<!ELEMENT CODE (#PCDATA)>
<!ELEMENT TEXT (#PCDATA)>
<!ELEMENT ITEM_LIST (ITEM+)>
<!ELEMENT ITEM (KEY, VALUE*)>
<!-- EOF -->
```

Option Profile Export

```
<!ELEMENT OPTION_PROFILES (OPTION_PROFILE)*>
<!ELEMENT OPTION_PROFILE (BASIC_INFO, SCAN, MAP?, ADDITIONAL,
INSTANCE_DATA_COLLECTION?,OS_BASED_INSTANCE_DISC_COLLECTION?)>
<!ELEMENT BASIC_INFO (ID, GROUP_NAME, GROUP_TYPE, USER_ID, UNIT_ID,
SUBSCRIPTION_ID, IS_DEFAULT?, IS_GLOBAL?, IS_OFFLINE_SYNCABLE?,
UPDATE_DATE?)>
<!ELEMENT ID (#PCDATA)>

<!ELEMENT GROUP_NAME (#PCDATA)>
```

```
<!ELEMENT GROUP_TYPE (#PCDATA)>
<!ELEMENT USER_ID (#PCDATA)>
<!ELEMENT UNIT_ID (#PCDATA)>
<!ELEMENT SUBSCRIPTION_ID (#PCDATA)>
<!ELEMENT IS_DEFAULT (#PCDATA)>
<!ELEMENT IS_GLOBAL (#PCDATA)>
<!ELEMENT IS_OFFLINE_SYNCABLE (#PCDATA)>
<!ELEMENT UPDATE_DATE (#PCDATA)>
<!ELEMENT SCAN (PORTS?, SCAN_DEAD_HOSTS?, CLOSE_VULNERABILITIES?,
PURGE_OLD_HOST_OS_CHANGED?, PERFORMANCE?, LOAD_BALANCER_DETECTION?,
PASSWORD_BRUTE_FORCING?, VULNERABILITY_DETECTION?, AUTHENTICATION?,
AUTHENTICATION_LEAST_PRIVILEGE?, ADDL_CERT_DETECTION?,
DISSOLVABLE_AGENT?, SCAN_RESTRICTION?, DATABASE_PREFERENCE_KEY?,
SYSTEM_AUTH_RECORD?, LITE_OS_SCAN?, CUSTOM_HTTP_HEADER?,
HOST_ALIVE_TESTING?, ETHERNET_IP_PROBING?, FILE_INTEGRITY_MONITORING?,
CONTROL_TYPES?, DO_NOT_OVERWRITE_OS?, TEST_AUTHENTICATION?,
MAX_SCAN_DURATION_PER_ASSET?, PERFORM_PARTIAL_SSL_TLS_AUDITING?)>

<!ELEMENT PORTS (TCP_PORTS?, UDP_PORTS?, AUTHORITATIVE_OPTION?,
(STANDARD_SCAN|TARGETED_SCAN)?)>

<!ELEMENT TCP_PORTS (TCP_PORTS_TYPE?, TCP_PORTS_STANDARD_SCAN?,
TCP_PORTS_ADDITIONAL?, THREE_WAY_HANDSHAKE?, STANDARD_SCAN?,
TCP_ADDITIONAL?)>

<!ELEMENT TCP_PORTS_TYPE (#PCDATA)>
<!ELEMENT TCP_PORTS_ADDITIONAL (HAS_ADDITIONAL?, ADDITIONAL_PORTS?)>
<!ELEMENT HAS_ADDITIONAL (#PCDATA)>
<!ELEMENT ADDITIONAL_PORTS (#PCDATA)>
<!ELEMENT THREE_WAY_HANDSHAKE (#PCDATA)>
<!ELEMENT UDP_PORTS (UDP_PORTS_TYPE?, UDP_PORTS_STANDARD_SCAN?,
UDP_PORTS_ADDITIONAL?, (STANDARD_SCAN|CUSTOM_PORT)?)>

<!ELEMENT UDP_PORTS_TYPE (#PCDATA)>
<!ELEMENT UDP_PORTS_ADDITIONAL (HAS_ADDITIONAL?, ADDITIONAL_PORTS?)>
<!ELEMENT AUTHORITATIVE_OPTION (#PCDATA)>
<!ELEMENT STANDARD_SCAN (#PCDATA)>
<!ELEMENT TARGETED_SCAN (#PCDATA)>
<!ELEMENT SCAN_DEAD_HOSTS (#PCDATA)>
<!ELEMENT CLOSE_VULNERABILITIES (HAS_CLOSE_VULNERABILITIES?,
HOST_NOT_FOUND_ALIVE?)>

<!ELEMENT HAS_CLOSE_VULNERABILITIES (#PCDATA)>
<!ELEMENT HOST_NOT_FOUND_ALIVE (#PCDATA)>
<!ELEMENT PURGE_OLD_HOST_OS_CHANGED (#PCDATA)>
<!ELEMENT PERFORMANCE (PARALLEL_SCALING?, OVERALL_PERFORMANCE,
HOSTS_TO_SCAN, PROCESSES_TO_RUN, PACKET_DELAY,
PORT_SCANNING_AND_HOST_DISCOVERY, EXTERNAL_SCANNERS_TO_USE?,
HOST_CGI_CHECKS?, MAX_CGI_CHECKS?, MAX_TARGETS_PER_SLICE?,
```

```
MAX_NUMBER_OF_TARGETS?, CONF_SCAN_LIMITED_CONNECTIVITY?,
SKIP_PRE_SCANNING?, SCAN_MULTIPLE_SLICES_PER_SCANNER?)>

<!ELEMENT PARALLEL_SCALING (#PCDATA)>
<!ELEMENT OVERALL_PERFORMANCE (#PCDATA)>
<!ELEMENT HOSTS_TO_SCAN (EXTERNAL_SCANNERS, SCANNER_APPLIANCES)>
<!ELEMENT EXTERNAL_SCANNERS (#PCDATA)>
<!ELEMENT SCANNER_APPLIANCES (#PCDATA)>
<!ELEMENT PROCESSES_TO_RUN (TOTAL_PROCESSES, HTTP_PROCESSES)>
<!ELEMENT TOTAL_PROCESSES (#PCDATA)>
<!ELEMENT HTTP_PROCESSES (#PCDATA)>
<!ELEMENT PACKET_DELAY (#PCDATA)>
<!ELEMENT PORT_SCANNING_AND_HOST_DISCOVERY (#PCDATA)>
<!ELEMENT EXTERNAL_SCANNERS_TO_USE (#PCDATA)>
<!ELEMENT HOST_CGI_CHECKS (#PCDATA)>
<!ELEMENT MAX_CGI_CHECKS (#PCDATA)>
<!ELEMENT MAX_TARGETS_PER_SLICE (#PCDATA)>
<!ELEMENT MAX_NUMBER_OF_TARGETS (#PCDATA)>
<!ELEMENT CONF_SCAN_LIMITED_CONNECTIVITY (#PCDATA)>
<!ELEMENT SKIP_PRE_SCANNING (#PCDATA)>
<!ELEMENT SCAN_MULTIPLE_SLICES_PER_SCANNER (#PCDATA)>
<!ELEMENT LOAD_BALANCER_DETECTION (#PCDATA)>
<!ELEMENT PASSWORD_BRUTE_FORCING (SYSTEM?, CUSTOM_LIST?)>
<!ELEMENT SYSTEM (HAS_SYSTEM?, SYSTEM_LEVEL?)>
<!ELEMENT HAS_SYSTEM (#PCDATA)>
<!ELEMENT SYSTEM_LEVEL (#PCDATA)>
<!ELEMENT CUSTOM_LIST (CUSTOM+)>
<!ELEMENT CUSTOM (ID, TITLE, TYPE?, LOGIN_PASSWORD?)+>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT TYPE (#PCDATA)>
<!ELEMENT LOGIN_PASSWORD (#PCDATA)>
<!ELEMENT MAX_SCAN_DURATION_PER_ASSET (#PCDATA)>
<!ELEMENT VULNERABILITY_DETECTION ((COMPLETE|CUSTOM_LIST|RUNTIME),
DETECTION_INCLUDE?, DETECTION_EXCLUDE?)>
<!ELEMENT COMPLETE (#PCDATA)>
<!ELEMENT RUNTIME (#PCDATA)>
<!ELEMENT DETECTION_INCLUDE (BASIC_HOST_INFO_CHECKS, OVAL_CHECKS,
QRDI_CHECKS?)>
<!ELEMENT BASIC_HOST_INFO_CHECKS (#PCDATA)>
<!ELEMENT OVAL_CHECKS (#PCDATA)>
<!ELEMENT QRDI_CHECKS (#PCDATA)>
<!ELEMENT DETECTION_EXCLUDE (CUSTOM_LIST+)>
<!ELEMENT AUTHENTICATION (#PCDATA)>
<!ELEMENT AUTHENTICATION_LEAST_PRIVILEGE (#PCDATA)>
<!ELEMENT ADDL_CERT_DETECTION (#PCDATA)>
<!ELEMENT DISSOLVABLE_AGENT (DISSOLVABLE_AGENT_ENABLE,
PASSWORD_AUDITING_ENABLE?, WINDOWS_SHARE_ENUMERATION_ENABLE,
WINDOWS_DIRECTORY_SEARCH_ENABLE?)>
```

```
<!ELEMENT DISSOLVABLE_AGENT_ENABLE (#PCDATA)>
<!ELEMENT PASSWORD_AUDITING_ENABLE (HAS_PASSWORD_AUDITING_ENABLE?,
CUSTOM_PASSWORD_DICTIONARY?)>
<!ELEMENT HAS_PASSWORD_AUDITING_ENABLE (#PCDATA)>
<!ELEMENT CUSTOM_PASSWORD_DICTIONARY (#PCDATA)>
<!ELEMENT WINDOWS_SHARE_ENUMERATION_ENABLE (#PCDATA)>
<!ELEMENT WINDOWS_DIRECTORY_SEARCH_ENABLE (#PCDATA)>
<!ELEMENT SCAN_RESTRICTION (SCAN_BY_POLICY?)>
<!ELEMENT SCAN_BY_POLICY  (POLICY+)>
<!ELEMENT POLICY (ID, TITLE)>
<!ELEMENT DATABASE_PREFERENCE_KEY (MSSQL?, ORACLE?, SYBASE?, POSTGRESQL?,
SAPIQ?, DB2?)>
<!ELEMENT MSSQL (DB_UDC_RESTRICTION, DB_UDC_LIMIT)>
<!ELEMENT ORACLE (DB_UDC_RESTRICTION, DB_UDC_LIMIT)>
<!ELEMENT SYBASE (DB_UDC_RESTRICTION, DB_UDC_LIMIT)>
<!ELEMENT POSTGRESQL (DB_UDC_RESTRICTION, DB_UDC_LIMIT)>
<!ELEMENT SAPIQ (DB_UDC_RESTRICTION, DB_UDC_LIMIT)>
<!ELEMENT DB2 (DB_UDC_RESTRICTION, DB_UDC_LIMIT)>
<!ELEMENT DB_UDC_RESTRICTION (#PCDATA)>
<!ELEMENT DB_UDC_LIMIT (#PCDATA)>
<!ELEMENT SYSTEM_AUTH_RECORD (ALLOW_AUTH_CREATION|INCLUDE_SYSTEM_AUTH)>
<!ELEMENT ALLOW_AUTH_CREATION (AUTHENTICATION_TYPE_LIST,
IBM_WAS_DISCOVERY_MODE?, ORACLE_AUTHENTICATION_TEMPLATE?,
MONGODB_AUTHENTICATION_TEMPLATE?)>
<!ELEMENT AUTHENTICATION_TYPE_LIST  (AUTHENTICATION_TYPE+)>
<!ELEMENT AUTHENTICATION_TYPE (#PCDATA)>
<!ELEMENT IBM_WAS_DISCOVERY_MODE  (#PCDATA)>
<!ELEMENT ORACLE_AUTHENTICATION_TEMPLATE  (ID, TITLE)>
<!ELEMENT MONGODB_AUTHENTICATION_TEMPLATE  (ID, TITLE)>
<!ELEMENT INCLUDE_SYSTEM_AUTH
(ON_DUPLICATE_USE_USER_AUTH|ON_DUPLICATE_USE_SYSTEM_AUTH)>
<!ELEMENT ON_DUPLICATE_USE_USER_AUTH (#PCDATA)>
<!ELEMENT ON_DUPLICATE_USE_SYSTEM_AUTH (#PCDATA)>
<!ELEMENT LITE_OS_SCAN (#PCDATA)>
<!ELEMENT CUSTOM_HTTP_HEADER (VALUE?, DEFINITION_KEY?,
DEFINITION_VALUE?)>
<!ELEMENT VALUE (#PCDATA)>
<!ELEMENT DEFINITION_KEY (#PCDATA)>
<!ELEMENT DEFINITION_VALUE (#PCDATA)>
<!ELEMENT HOST_ALIVE_TESTING (#PCDATA)>
<!ELEMENT ETHERNET_IP_PROBING (#PCDATA)>
<!ELEMENT FILE_INTEGRITY_MONITORING (AUTO_UPDATE_EXPECTED_VALUE?)>
<!ELEMENT AUTO_UPDATE_EXPECTED_VALUE (#PCDATA)>
<!ELEMENT CONTROL_TYPES (FIM_CONTROLS_ENABLED?,
CUSTOM_WMI_QUERY_CHECKS?)>
<!ELEMENT FIM_CONTROLS_ENABLED (#PCDATA)>
<!ELEMENT CUSTOM_WMI_QUERY_CHECKS (#PCDATA)>

<!ELEMENT DO_NOT_OVERWRITE_OS (#PCDATA)>
```

```
<!ELEMENT TEST_AUTHENTICATION (#PCDATA)>
<!ELEMENT PERFORM_PARTIAL_SSL_TLS_AUDITING (#PCDATA)>
<!ELEMENT MAP (BASIC_INFO_GATHERING_ON, TCP_PORTS?, UDP_PORTS?,
MAP_OPTIONS?, MAP_PERFORMANCE?, MAP_AUTHENTICATION?)>
<!ELEMENT BASIC_INFO_GATHERING_ON (#PCDATA)>
<!ELEMENT TCP_PORTS_STANDARD_SCAN (#PCDATA)>
<!ELEMENT UDP_PORTS_STANDARD_SCAN (#PCDATA)>
<!ELEMENT MAP_OPTIONS (PERFORM_LIVE_HOST_SWEEP?,  DISABLE_DNS_TRAFFIC?)>
<!ELEMENT PERFORM_LIVE_HOST_SWEEP (#PCDATA)>
<!ELEMENT DISABLE_DNS_TRAFFIC (#PCDATA)>
<!ELEMENT MAP_PERFORMANCE (OVERALL_PERFORMANCE, MAP_PARALLEL?,
PACKET_DELAY)>
<!ELEMENT MAP_PARALLEL (EXTERNAL_SCANNERS, SCANNER_APPLIANCES,
NETBLOCK_SIZE)>
<!ELEMENT NETBLOCK_SIZE (#PCDATA)>
<!ELEMENT MAP_AUTHENTICATION (#PCDATA)>
<!ELEMENT ADDITIONAL (HOST_DISCOVERY, BLOCK_RESOURCES?, PACKET_OPTIONS?)>
<!ELEMENT HOST_DISCOVERY (TCP_PORTS?, UDP_PORTS?, ICMP?)>
<!ELEMENT TCP_ADDITIONAL (HAS_ADDITIONAL?, ADDITIONAL_PORTS?)>
<!ELEMENT CUSTOM_PORT (#PCDATA)>
<!ELEMENT ICMP (#PCDATA)>
<!ELEMENT BLOCK_RESOURCES
((WATCHGUARD_DEFAULT_BLOCKED_PORTS|CUSTOM_PORT_LIST),
(ALL_REGISTERED_IPS|CUSTOM_IP_LIST))>
<!ELEMENT WATCHGUARD_DEFAULT_BLOCKED_PORTS (#PCDATA)>
<!ELEMENT CUSTOM_PORT_LIST (#PCDATA)>
<!ELEMENT ALL_REGISTERED_IPS (#PCDATA)>
<!ELEMENT CUSTOM_IP_LIST (#PCDATA)>
<!ELEMENT PACKET_OPTIONS (IGNORE_FIREWALL_GENERATED_TCP_RST?,
IGNORE_ALL_TCP_RST?,  IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK?,
NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY?)>
<!ELEMENT IGNORE_FIREWALL_GENERATED_TCP_RST (#PCDATA)>
<!ELEMENT IGNORE_ALL_TCP_RST (#PCDATA)>
<!ELEMENT IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK (#PCDATA)>
<!ELEMENT NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY (#PCDATA)>
<!ELEMENT INSTANCE_DATA_COLLECTION (DATABASES?)>
<!ELEMENT DATABASES (AUTHENTICATION_TYPES_LIST)>
<!ELEMENT AUTHENTICATION_TYPES_LIST  (AUTHENTICATION_TYPE+)>
<!ELEMENT OS_BASED_INSTANCE_DISC_COLLECTION (TECHNOLOGIES?)>
<!ELEMENT TECHNOLOGIES (TECHNOLOGY+)>
<!ELEMENT TECHNOLOGY  (#PCDATA)>
```

Filter Vulnerabilities Based on their Type

APIs affected	/api/2.0/fo/asset/host/vm/detection/
New or Updated API	Updated
DTD or XSD changes	No

With this release, to optimize the vulnerability information download process, a new filter parameter has been introduced. It enables to filter vulnerability information based on vulnerability types, confirmed, and potential vulnerabilities. You can now download only confirmed or only potential vulnerabilities as per your business requirement. This optimizes the vulnerability information download process by eliminating vulnerabilities you don't want to focus on and process.

Input Parameter

The following new parameter is added to the request. This is an optional parameter.

Parameter	Description
include_vuln_type	Use to download vulnerability information based on their type, confirmed or potential. Specify: • `include_vuln_type=confirmed` to download only confirmed vulnerabilities. • `include_vuln_type=potential` to download only potential vulnerabilities.

Exceptional Scenarios

- After passing the parameter value `include_vuln_type=confirmed`, some potential vulnerabilities may show up in the API response. This happens when the vulnerability type for the QID is modified in the Qualys KnowledgeBase.
- After passing the parameter value `include_vuln_type=potential`, some confirmed vulnerabilities show up in the API response.
  - This happens with the vulnerabilities assigned with a half red/half yellow severity level.
  - This happens when the vulnerability type for the QID is changed while running the authenticated scan. It is because of various factors affecting scan results.

API Sample

Sample - Download a list of hosts with the latest vulnerability data, based on vulnerability type, confirmed

API Request:

```
curl --location
'<qualys_base_url>/api/2.0/fo/asset/host/vm/detection/?action=list&ips=11
.111.11.111&include_vuln_type=confirmed' \

--header 'X-Requested-With: curl'

--header 'Authorization: Basic <encoded username:password string>'
```

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>2023-08-16T13:34:18Z</DATETIME>
        <HOST_LIST>
            <HOST>
                <ID>524323</ID>
                <IP>11.111.11.111</IP>
                <TRACKING_METHOD>IP</TRACKING_METHOD>
                <OS>
                   <![CDATA[Linux 2.4-2.6 / Embedded Device / F5 Networks
Big-IP]]>
                </OS>
                <LAST_SCAN_DATETIME>2019-11-
08T09:15:14Z</LAST_SCAN_DATETIME>
                <LAST_VM_SCANNED_DATE>2019-11-
08T06:37:29Z</LAST_VM_SCANNED_DATE>
                <DETECTION_LIST>
                    <DETECTION>
                        <UNIQUE_VULN_ID>3978355</UNIQUE_VULN_ID>
                        <QID>82054</QID>
                        <TYPE>Confirmed</TYPE>
                        <SEVERITY>2</SEVERITY>
                        <SSL>0</SSL>
                        <RESULTS>
                            <![CDATA[Tested on port 2222 with an injected
SYN/RST offset by 16 bytes.]]>
                        </RESULTS>
```

```
                        <STATUS>New</STATUS>
                        <FIRST_FOUND_DATETIME>2019-11-
08T06:37:29Z</FIRST_FOUND_DATETIME>
                        <LAST_FOUND_DATETIME>2019-11-
08T06:37:29Z</LAST_FOUND_DATETIME>
                        <TIMES_FOUND>1</TIMES_FOUND>
                        <LAST_TEST_DATETIME>2019-11-
08T06:37:29Z</LAST_TEST_DATETIME>
                        <LAST_UPDATE_DATETIME>2019-11-
08T09:15:14Z</LAST_UPDATE_DATETIME>
                        <IS_IGNORED>0</IS_IGNORED>
                        <IS_DISABLED>0</IS_DISABLED>
                        <LAST_PROCESSED_DATETIME>2019-11-
08T09:15:14Z</LAST_PROCESSED_DATETIME>
                    </DETECTION>
                </DETECTION_LIST>
            </HOST>
        </HOST_LIST>
    </RESPONSE>
</HOST_LIST_VM_DETECTION_OUTPUT>
```

API Sample

Sample - Download a list of hosts with the latest vulnerability data, based on vulnerability type, potential

API Request:

```
curl --location
'<qualys_base_url>/api/2.0/fo/asset/host/vm/detection/?action=list&ips=11
.110.11.111&include_vuln_type=potential' \
--header 'X-Requested-With: curl'
--header 'Authorization: Basic <encoded username:password string>'
```

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>2023-08-16T11:51:13Z</DATETIME>
        <HOST_LIST>
            <HOST>
                <ID>524323</ID>
                <IP>11.110.11.111</IP>
                <TRACKING_METHOD>IP</TRACKING_METHOD>
                <OS>
                   <![CDATA[Linux 2.4-2.6 / Embedded Device / F5 Networks
Big-IP]]>
```

```
                </OS>
                <LAST_SCAN_DATETIME>2019-11-
08T09:15:14Z</LAST_SCAN_DATETIME>
                <LAST_VM_SCANNED_DATE>2019-11-
08T06:37:29Z</LAST_VM_SCANNED_DATE>
                <DETECTION_LIST>
                    <DETECTION>
                        <UNIQUE_VULN_ID>3978356</UNIQUE_VULN_ID>
                        <QID>38469</QID>
                        <TYPE>Potential</TYPE>
                        <SEVERITY>2</SEVERITY>
                        <SSL>0</SSL>
                        <RESULTS>
                            <![CDATA[SSH-2.0-OpenSSH_3.9p1-AuthSelect-
SecurID-log]]>
                        </RESULTS>
                        <STATUS>New</STATUS>
                        <FIRST_FOUND_DATETIME>2019-11-
08T06:37:29Z</FIRST_FOUND_DATETIME>
                        <LAST_FOUND_DATETIME>2019-11-
08T06:37:29Z</LAST_FOUND_DATETIME>
                        <TIMES_FOUND>1</TIMES_FOUND>
                        <LAST_TEST_DATETIME>2019-11-
08T06:37:29Z</LAST_TEST_DATETIME>
                        <LAST_UPDATE_DATETIME>2019-11-
08T09:15:14Z</LAST_UPDATE_DATETIME>
                        <IS_IGNORED>0</IS_IGNORED>
                        <IS_DISABLED>0</IS_DISABLED>
                        <LAST_PROCESSED_DATETIME>2019-11-
08T09:15:14Z</LAST_PROCESSED_DATETIME>
                    </DETECTION>
                    <DETECTION>
                        <UNIQUE_VULN_ID>3978354</UNIQUE_VULN_ID>
                        <QID>38560</QID>
                        <TYPE>Potential</TYPE>
                        <SEVERITY>4</SEVERITY>
                        <SSL>0</SSL>
                        <RESULTS>
                            <![CDATA[SSH-2.0-OpenSSH_3.9p1-AuthSelect-
SecurID-log]]>
                        </RESULTS>
                        <STATUS>New</STATUS>
                        <FIRST_FOUND_DATETIME>2019-11-
08T06:37:29Z</FIRST_FOUND_DATETIME>
                        <LAST_FOUND_DATETIME>2019-11-
08T06:37:29Z</LAST_FOUND_DATETIME>
                        <TIMES_FOUND>1</TIMES_FOUND>
                        <LAST_TEST_DATETIME>2019-11-
08T06:37:29Z</LAST_TEST_DATETIME>
```

```
                        <LAST_UPDATE_DATETIME>2019-11-
08T09:15:14Z</LAST_UPDATE_DATETIME>
                        <IS_IGNORED>0</IS_IGNORED>
                        <IS_DISABLED>0</IS_DISABLED>
                        <LAST_PROCESSED_DATETIME>2019-11-
08T09:15:14Z</LAST_PROCESSED_DATETIME>
                    </DETECTION>
                    <DETECTION>
                        <UNIQUE_VULN_ID>3978353</UNIQUE_VULN_ID>
                        <QID>115317</QID>
                        <TYPE>Potential</TYPE>
                        <SEVERITY>3</SEVERITY>
                        <SSL>0</SSL>
                        <RESULTS>
                            <![CDATA[SSH-2.0-OpenSSH_3.9p1-AuthSelect-
SecurID-log]]>
                        </RESULTS>
                        <STATUS>New</STATUS>
                        <FIRST_FOUND_DATETIME>2019-11-
08T06:37:29Z</FIRST_FOUND_DATETIME>
                        <LAST_FOUND_DATETIME>2019-11-
08T06:37:29Z</LAST_FOUND_DATETIME>
                        <TIMES_FOUND>1</TIMES_FOUND>
                        <LAST_TEST_DATETIME>2019-11-
08T06:37:29Z</LAST_TEST_DATETIME>
                        <LAST_UPDATE_DATETIME>2019-11-
08T09:15:14Z</LAST_UPDATE_DATETIME>
                        <IS_IGNORED>0</IS_IGNORED>
                        <IS_DISABLED>0</IS_DISABLED>
                        <LAST_PROCESSED_DATETIME>2019-11-
08T09:15:14Z</LAST_PROCESSED_DATETIME>
                    </DETECTION>
                </DETECTION_LIST>
            </HOST>
        </HOST_LIST>
    </RESPONSE>
</HOST_LIST_VM_DETECTION_OUTPUT>
```