Qualys Cloud Platform (VM, PC) v10.x

API Release Notes

Version 10.20.1

August 1, 2022

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

Run Vulnerability Scans using Least Privilege for Unix Authentication

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.

Run Vulnerability Scans using Least Privilege for Unix Authentication

APIs affected	/api/2.0/fo/subscription/option_profile/vm/?action=create|update /api/2.0/fo/subscription/option_profile/vm/?action=list /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

We've added a new scan option in the vulnerability option profile that allows users to specify that they want to use the least privileges required for Unix authentication. To use this option, specify the new input parameter **authentication_least_privilege=Unix** in the API request when creating or updating an option profile. When specified, we will not pass root delegation information from the Unix authentication record to the scanner during vulnerability scans, and thus the scanner will not perform checks with elevated privileges that are not required.

Purpose and Benefit

For compliance scans, in order to evaluate all compliance checks an account with superuser (root) privileges is required. Users have the option in the Unix authentication record to use root delegation tools (Sudo, Pimsu, PowerBroker) in order to provide a lower-privileged user account in the record and still perform scan tests with the elevated privileges of the superuser (root).

For vulnerability scans, root level privileges are not mandatory. However, since the same authentication records are used for both compliance scans and vulnerability scans, root level privileges are being used for vulnerability scans when root delegation tools are selected in the Unix record.

The principle of least privilege access is a security best practice where only the minimum account privileges required are used to perform an action. It's for this reason that we've introduced this new scan option for vulnerability scans. When this new option is used, we will not pass the root delegation information specified in the Unix record to the scanner for vulnerability scans. The lower privileged user account specified in the Unix record will be used for the host authentication. There will be no change to compliance scans and root delegation will be used for compliance scans when specified in the Unix authentication record.

The authentication records you already have set up in your account will continue to work for both vulnerability scans and compliance scans. Using the new least privilege authentication option simply means the root delegation settings in the Unix record will not be used for vulnerability scans.

Create/Update Option Profile

We added a new input parameter for the VM option profile for enabling Unix authentication with least privilege.

Input Parameters

Use this new input parameter when creating or editing a VM option profile. Refer to the Qualys API (VM,PC) User Guide for details on all available input parameters.

Parameter	Description
authentication_least_privilege=Unix	(Optional to create or update option profile) Specify authentication_least_privilege=Unix (this value is case sensitive) to use the least privileges required for Unix authentication. When specified, the scanner will not pass root delegation information specified in the Unix record to the scanner for vulnerability scans. When not specified (the default), root delegation will be used if specified in the Unix record. Note: Unix authentication must be enabled in the same option profile (authentication=Unix).

Sample Create Option Profile

In this sample, we're creating a new option profile with authentication least privileges.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST
"action=create&title=unix least
privilege&scan_tcp_ports=standard&scan_udp_ports=standard&vulnerability_d
etection=complete&basic_information_gathering=all&map_tcp_ports_standard_
scan=1&authentication=Unix&authentication_least_privilege=Unix"
"http://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/vm/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"http://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2022-07-27T07:58:36Z</DATETIME>
        <TEXT>Option profile successfully added.</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>144975</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Sample Update Option Profile

In this sample, we're updating an existing option profile with authentication least privileges.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST
"action=update&id=123456&title=least privilege
auth&authentication=Unix&authentication_least_privilege=Unix"
"http://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/vm/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"http://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2022-07-27T09:08:12Z</DATETIME>
        <TEXT>Option profile successfully updated.</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>123456</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

List Option Profile

In this sample, we are listing a single option profile specified by the profile ID. In the XML output, you'll see the new tag AUTHENTICATION_LEAST_PRIVILEGE when enabled.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X GET
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/vm/?
action=list&id=144961"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM
"http://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/optio
n_profile_info.dtd">
<OPTION_PROFILES>
    <OPTION_PROFILE>
        <BASIC_INFO>
            <ID>123456</ID>
```

```
                <GROUP_NAME>
                    <![CDATA[least privilege auth]]>
                </GROUP_NAME>
                <GROUP_TYPE>user</GROUP_TYPE>
                <USER_ID>
                    <![CDATA[Joe User (joe_user)]]>
                </USER_ID>
                <UNIT_ID>0</UNIT_ID>
                <SUBSCRIPTION_ID>123456</SUBSCRIPTION_ID>
                <IS_DEFAULT>0</IS_DEFAULT>
                <IS_GLOBAL>0</IS_GLOBAL>
                <IS_OFFLINE_SYNCABLE>0</IS_OFFLINE_SYNCABLE>
                <UPDATE_DATE>2022-07-27T09:08:12Z</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[Unix]]>
            </AUTHENTICATION>
            <AUTHENTICATION_LEAST_PRIVILEGE>
                <![CDATA[Unix]]>
            </AUTHENTICATION_LEAST_PRIVILEGE>
            <ADDL_CERT_DETECTION>0</ADDL_CERT_DETECTION>
            <DISSOLVABLE_AGENT>
                <DISSOLVABLE_AGENT_ENABLE>0</DISSOLVABLE_AGENT_ENABLE>

<WINDOWS_SHARE_ENUMERATION_ENABLE>0</WINDOWS_SHARE_ENUMERATION_ENABLE>
            </DISSOLVABLE_AGENT>
        </SCAN>
...
```

Export Option Profile

In this sample, we're exporting all option profiles in the account. You'll see AUTHENTICATION_LEAST_PRIVILEGE for option profiles with this setting enabled. The first option profile in the sample below does not have the setting. The second option profile in the sample does have the setting.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X GET
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/?act
ion=export"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM
"http://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/optio
n_profile_info.dtd">
<OPTION_PROFILES>
    <OPTION_PROFILE>
        <BASIC_INFO>
            <ID>135325</ID>
            <GROUP_NAME>
                <![CDATA[Sample Option Profile 1]]>
            </GROUP_NAME>
            <GROUP_TYPE>user</GROUP_TYPE>
            <USER_ID>
                <![CDATA[Joe User (joe_user)]]>
            </USER_ID>
            <UNIT_ID>0</UNIT_ID>
```

```
                <SUBSCRIPTION_ID>123456</SUBSCRIPTION_ID>
                <IS_DEFAULT>0</IS_DEFAULT>
                <IS_GLOBAL>0</IS_GLOBAL>
                <IS_OFFLINE_SYNCABLE>0</IS_OFFLINE_SYNCABLE>
                <UPDATE_DATE>2022-07-27T05:19:16Z</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,MongoDB,VMware]]>
                </AUTHENTICATION>
                <ADDL_CERT_DETECTION>0</ADDL_CERT_DETECTION>
...
```

```
    </OPTION_PROFILE>
    <OPTION_PROFILE>
        <BASIC_INFO>
            <ID>144974</ID>
            <GROUP_NAME>
                <![CDATA[Sample Option Profile 2]]>
            </GROUP_NAME>
            <GROUP_TYPE>user</GROUP_TYPE>
            <USER_ID>
                <![CDATA[Joe User (joe_user)]]>
            </USER_ID>
            <UNIT_ID>0</UNIT_ID>
            <SUBSCRIPTION_ID>123456</SUBSCRIPTION_ID>
            <IS_DEFAULT>0</IS_DEFAULT>
            <IS_GLOBAL>0</IS_GLOBAL>
            <IS_OFFLINE_SYNCABLE>0</IS_OFFLINE_SYNCABLE>
            <UPDATE_DATE>2022-07-26T18:21:00Z</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[Unix]]>
            </AUTHENTICATION>
            <AUTHENTICATION_LEAST_PRIVILEGE>
                <![CDATA[Unix]]>
            </AUTHENTICATION_LEAST_PRIVILEGE>
            <ADDL_CERT_DETECTION>0</ADDL_CERT_DETECTION>
            <DISSOLVABLE_AGENT>
                <DISSOLVABLE_AGENT_ENABLE>0</DISSOLVABLE_AGENT_ENABLE>

<WINDOWS_SHARE_ENUMERATION_ENABLE>0</WINDOWS_SHARE_ENUMERATION_ENABLE>
            </DISSOLVABLE_AGENT>
        </SCAN>
...
```

Import Option Profile

In this sample, we're importing an option profile from an XML file to the user's account.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -H "content-type:
text/xml" -X POST --data-binary @Export_OP.xml
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/?act
ion=import"
```

Note: The Export_OP.xml file contains the request POST data.

Request POST Data:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/opti
on_profile_info.dtd">
<OPTION_PROFILES>
    <OPTION_PROFILE>
        <BASIC_INFO>
            <ID>123456</ID>
            <GROUP_NAME>
                <![CDATA[least privilege auth]]>
            </GROUP_NAME>
            <GROUP_TYPE>user</GROUP_TYPE>
            <USER_ID>
```

```
                    <![CDATA[Joe User (joe_user)]]>
                </USER_ID>
                <UNIT_ID>0</UNIT_ID>
                <SUBSCRIPTION_ID>123456</SUBSCRIPTION_ID>
                <IS_DEFAULT>0</IS_DEFAULT>
                <IS_GLOBAL>0</IS_GLOBAL>
                <IS_OFFLINE_SYNCABLE>0</IS_OFFLINE_SYNCABLE>
                <UPDATE_DATE>N/A</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[Unix]]>
```

```
                </AUTHENTICATION>
                <AUTHENTICATION_LEAST_PRIVILEGE>
                    <![CDATA[Unix]]>
                </AUTHENTICATION_LEAST_PRIVILEGE>
                <ADDL_CERT_DETECTION>0</ADDL_CERT_DETECTION>
                <DISSOLVABLE_AGENT>
                    <DISSOLVABLE_AGENT_ENABLE>0</DISSOLVABLE_AGENT_ENABLE>

<WINDOWS_SHARE_ENUMERATION_ENABLE>0</WINDOWS_SHARE_ENUMERATION_ENABLE>
                </DISSOLVABLE_AGENT>
            </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>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>
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
 <RESPONSE>
   <DATETIME>2022-07-27T09:08:12Z</DATETIME>
   <TEXT>Successfully imported Option profile for the subscription Id
123456</TEXT>
   <ITEM_LIST>
     <ITEM>
       <KEY>144975</KEY>
       <VALUE>New Option Profile</VALUE>
     </ITEM>
  </ITEM_LIST>
 </RESPONSE>
</SIMPLE_RETURN>
```

Option Profile Info DTD Update

The Option Profile Info DTD was updated to include the new element AUTHENTICATION_LEAST_PRIVILEGE (in bold).

DTD: <platform>/api/2.0/fo/subscription/option_profile/option_profile_info.dtd

```
<!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?)>

<!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)>
...
```