Qualys Cloud Platform (VM, PC) 10.x

Release Notes

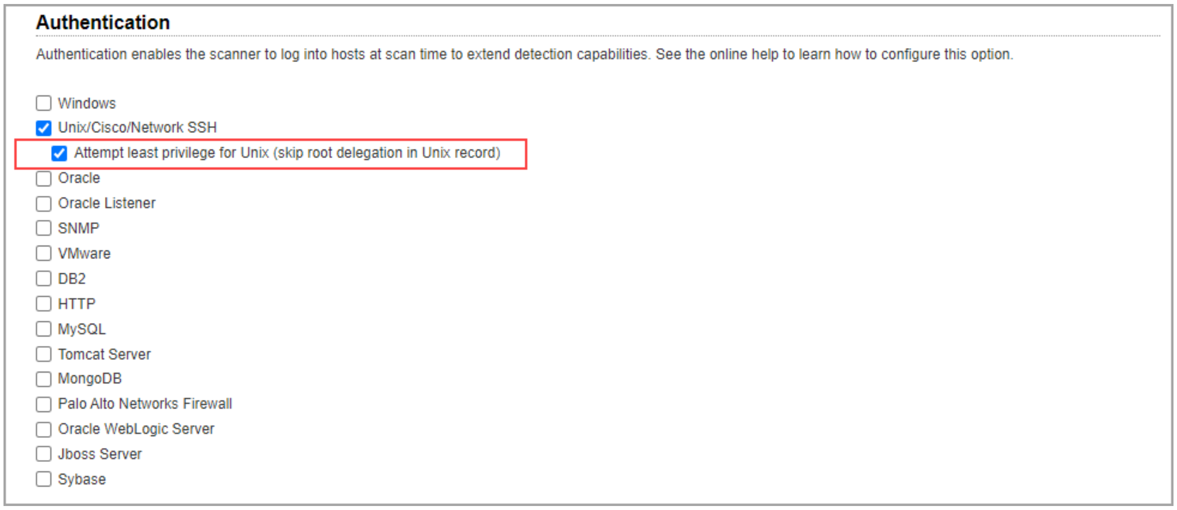
Version 10.20.1
August 4, 2022

This new release of the Qualys Cloud Platform (VM, PC) includes the following improvement to Vulnerability Management.

Attempt Least Privilege for Unix

The vulnerability option profile includes a new scan option that allows users to attempt least privileges required when using Unix authentication.

Go to **VM/VMDR** > **Scans** > **Option Profiles**. On the **Scan** tab, scroll down to the **Authentication** section. Enable Unix authentication, and then select **Attempt least privilege for Unix (skip root delegation in Unix record)**.



Authentication

Authentication enables the scanner to log into hosts at scan time to extend detection capabilities. See the online help to learn how to configure this option.

- □ Windows
- ☑ Unix/Cisco/Network SSH
  - ☑ Attempt least privilege for Unix (skip root delegation in Unix record)
- □ Oracle
- □ Oracle Listener
- □ SNMP
- □ VMware
- □ DB2
- □ HTTP
- □ MySQL
- □ Tomcat Server
- □ MongoDB
- □ Palo Alto Networks Firewall
- □ Oracle WebLogic Server
- □ Jboss Server
- □ Sybase

When the option **Attempt least privilege for Unix (skip root delegation in Unix record)** is selected in the option profile, we will not pass root delegation information from Unix authentication records to the scanner during vulnerability scans, and thus the scanner will not perform checks with elevated root 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 introduced this scan option for vulnerability scans. When this 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. This option will not affect compliance scans.