Qualys Cloud Platform v3.x Release Notes

Version 3.3.1
December 03, 2020 (updated on December 22, 2020)

Here's what's new in Qualys Cloud Suite 3.3.1!

VMDR Vulnerability Management Detection and Response

Auto-update of Asset Name

New RTI and Search Token for Solorigate Sunburst

UD Unified Dashboard

New Templates for FireEye and Solorigate/Sunburst

Qualys Cloud Platform 3.3.1 brings you many more Improvements and updates! Learn more

Vulnerability Management Detection and Response

Auto-update of Asset Name

You can now configure assets to be automatically renamed when a key attribute such as DNS, NETBIOS,INSTANCE_ID, IP address associated with an asset is updated.

A host asset name is derived based on the key attributes (such as DNS, NETBIOS,INSTANCE_ID, IP address). If an attribute name changes, then it did not automatically reflect in the host asset name. Users had to manually rename such host assets. To avoid this manual and tedious task, you can enable and use the automatic update feature.

Note: The automatic update for asset name is an optional feature and is disabled by default. To enable this feature for your subscription, please contact Qualys Support.

Once you enable the feature, the asset name is automatically updated across your enterprise, whenever any key attribute (such as DNS, NETBIOS,INSTANCE_ID, IP address) changes.

Disable Auto-Update of Assets

Once you enable this feature, the host asset name is automatically updated whenever any of the key attribute changes. If you want to disable automatic update of certain assets , you can simply rename the asset name.

Go to Assets > Assets tab, select the asset to be renamed. From the quick actions menu, select View Asset Details. On the Asset Summary pane, click Rename link to rename the asset. Once you manually rename an asset, the automatic update of assets are disabled for the asset.

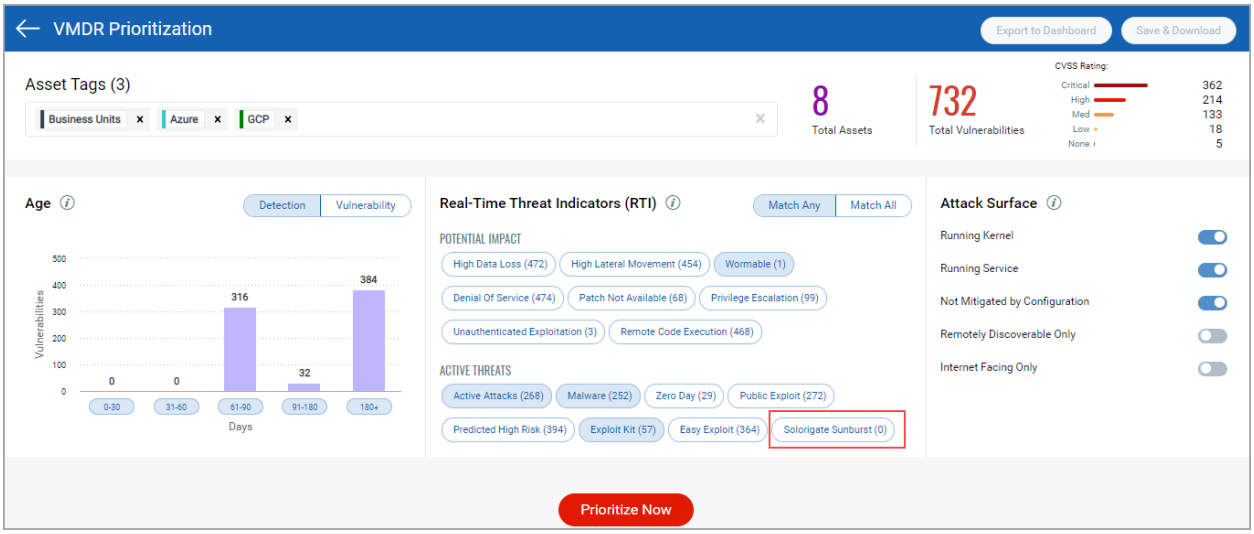
You can enable the automatic update of assets again. Select the Auto-update Asset check box to enable the feature for the asset.

Note: The Auto-update Asset check box is available to enable the automatic update of assets only after you manually rename the asset and disable the feature.

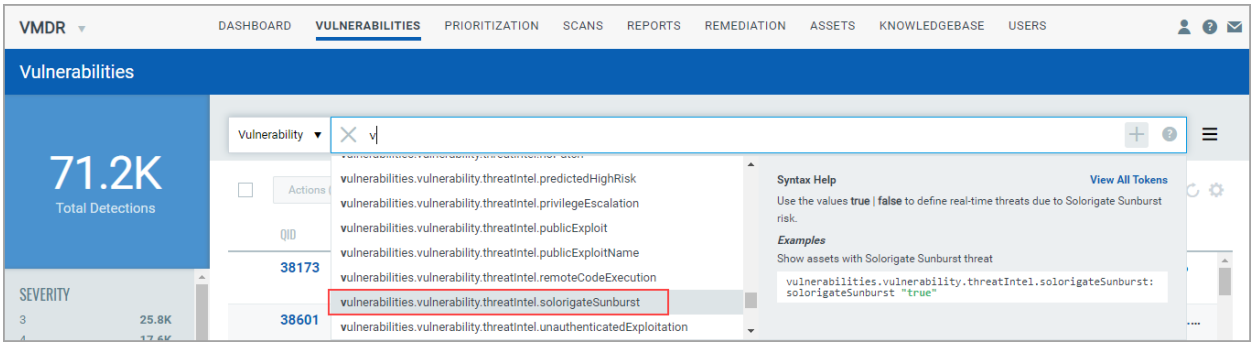
New RTI and Search Token for Solorigate/Sunburst

We have now introduced a new Real-Time Threat Indicator (RTI), Solorigate Sunburst, to help you quickly prioritize assets that could be vulnerable to the Solorigate/Sunburst threat.

When you generate prioritization report, in the RTI section, you can notice the new RTI available for selection.



Use our new search token `vulnerabilities.vulnerability.threatIntel.solorigateSunburst` to simplify your search for assets exposed to the Solorigate/Sunburst vulnerability.



UD Unified Dashboard

New Templates for FireEye and Solorigate/Sunburst

We have now updated our template library with two new templates to include the latest FireEye and Solorigate/Sunburst related threats. You can use these pre-defined template dashboards to have a single-pane-of-glass view on the dashboard for assets with specific areas of concern.

The new templates that we have introduced in this release are:

- **FireEye Theft | TOP 16 CVES & 50+ IOC Hashes** – Provides you with the TOP 16 CVEs and 50+ IOC Hashes for FireEye Breach.
- **FireEye RedTeam Tools & Solorigate/Sunburst** – Provides you with the vulnerabilities for Solorigate/Sunburst.

Issues Addressed

We have fixed the following issues in this current release-

AV AssetView

- We have now reverted the change that marked the cloud agent as "TERMINATED" or "DELETED" if the cloud agent on AWS and Microsoft Azure assets did not communicate for 24 hours.
- We have fixed an issue where Microsoft Azure VM instances encountered error during connector processing. As a result, the connector is stuck with "synchronized" status. This mainly affects VM instances, which had a cloud agent deployed on it, but the agent has been uninstalled/purged and connector continues to discover the instance.