Qualys Cloud Platform v3.x

Release Notes

Version 3.12.1

August 1, 2022

Here's what's new in Qualys Cloud Suite 3.12.1!

CA Cloud Agent

Column Name Changes in Asset Details – Open Ports

VM Scan Mode for Qualys Agent

VMDR Vulnerability Management, Detection, and Response

Detect and Patch the PwnKit Vulnerability

New PWNKIT Dashboard Template

CISA Vulns Renamed in Vulnerabilities Tab

New Data Fields for Asset and Vulnerability Report

New Global TLS Protocol Insights Dashboard Template

Updated Tokens for VMDR

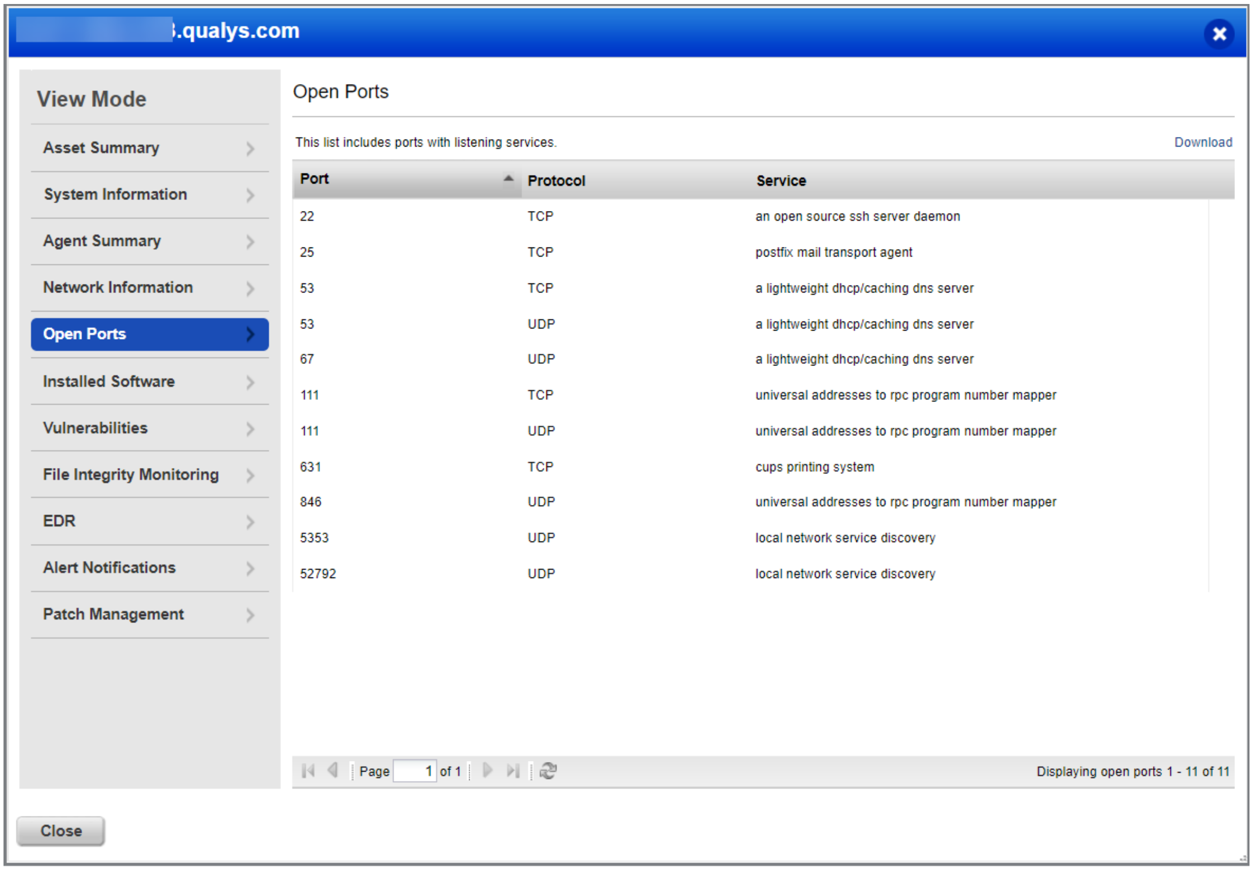
Qualys Cloud Platform 3.12.1 brings you many more improvements and updates! Learn more

CA Cloud Agent

Column Name Changes in Asset Details – Open Ports

With this release, we have made the following changes to the **Open Ports** information that is displayed when you select an agent and click **View Asset Details** from **Quick Actions**:

- Renamed the **Detected Service** column to **Service**.
- Deleted the **Service Description** column.



[redacted].qualys.com

Open Ports

This list includes ports with listening services.

Port	Protocol	Service
22	TCP	an open source ssh server daemon
25	TCP	postfix mail transport agent
53	TCP	a lightweight dhcp/caching dns server
53	UDP	a lightweight dhcp/caching dns server
67	UDP	a lightweight dhcp/caching dns server
111	TCP	universal addresses to rpc program number mapper
111	UDP	universal addresses to rpc program number mapper
631	TCP	cups printing system
846	UDP	universal addresses to rpc program number mapper
5353	UDP	local network service discovery
52792	UDP	local network service discovery

Displaying open ports 1 - 11 of 11

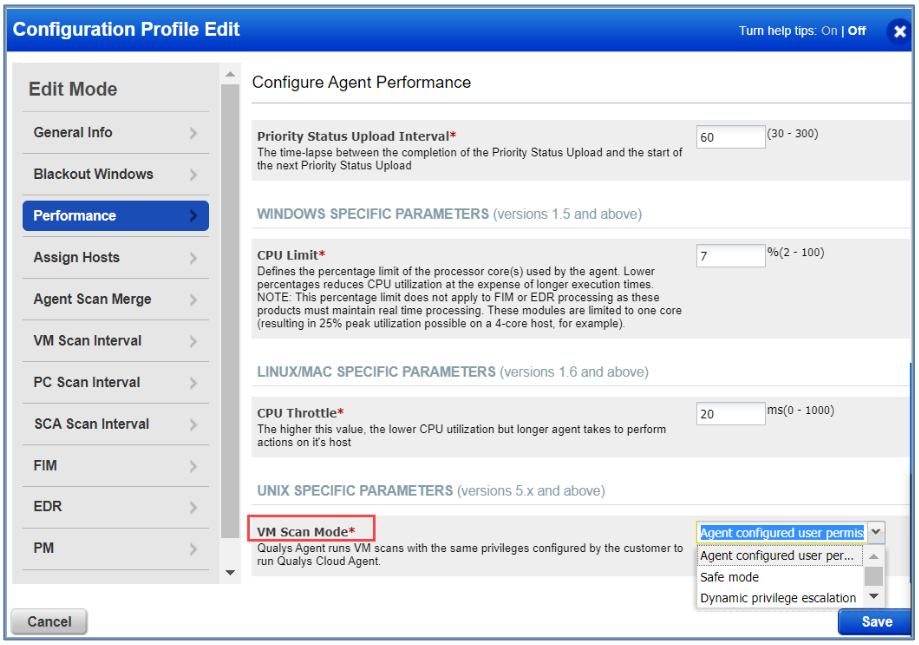
VM Scan Mode for Qualys Agent

The latest release provides different modes, where you can select the different privileges to run VM scan. Based on the settings you configure, the Qualys Agent scan is performed in one of the following modes:

- **Agent configured user permissions**: Qualys Agent runs VM scan with the same privileges configured by the customer to run Qualys Agent.
- **Safe mode**: Qualys Agent runs the VM scan only with lower privileges and would not run any commands/binary with elevated privileges.
- **Dynamic privilege elevation**: By default, Qualys Agent runs the VM scan with lower privileges. However, the Cloud Agent will dynamically elevate the privileges to root access only for those commands that failed due to permissions with lower privileges.

To enable the VM Scan Mode:

1. Go to **Configuration Profiles** > **Performance**.
2. Turn on the **Customize** toggle button to enable the settings.
3. Scroll to the **UNIX SPECIFIC PARAMETERS** section and select the required option from the drop-down menu.



Configure Agent Performance

Priority Status Upload Interval* 60 (30 - 300)
The time-lapse between the completion of the Priority Status Upload and the start of the next Priority Status Upload

WINDOWS SPECIFIC PARAMETERS (versions 1.5 and above)

CPU Limit* 7 %(2 - 100)
Defines the percentage limit of the processor core(s) used by the agent. Lower percentages reduces CPU utilization at the expense of longer execution times. NOTE: This percentage limit does not apply to FIM or EDR processing as these products must maintain real time processing. These modules are limited to one core (resulting in 25% peak utilization possible on a 4-core host, for example).

LINUX/MAC SPECIFIC PARAMETERS (versions 1.6 and above)

CPU Throttle* 20 ms(0 - 1000)
The higher this value, the lower CPU utilization but longer agent takes to perform actions on it's host

UNIX SPECIFIC PARAMETERS (versions 5.x and above)

VM Scan Mode* Agent configured user permis
Qualys Agent runs VM scans with the same privileges configured by the customer to run Qualys Cloud Agent.

Agent configured user per...
Safe mode
Dynamic privilege escalation

The default settings are as follows:

- By default, the **Customize** toggle button is turned off. To enable the **VM Scan Mode**, you need to enable the **Customize** toggle button.

Note: Even if the **Customize** toggle button is turned off, the configuration profile will have the Agent User privileges enabled.

- By default, when the Customize toggle button is turned on, the **Agent User** option is selected in the **VM Scan Mode** drop-down menu.

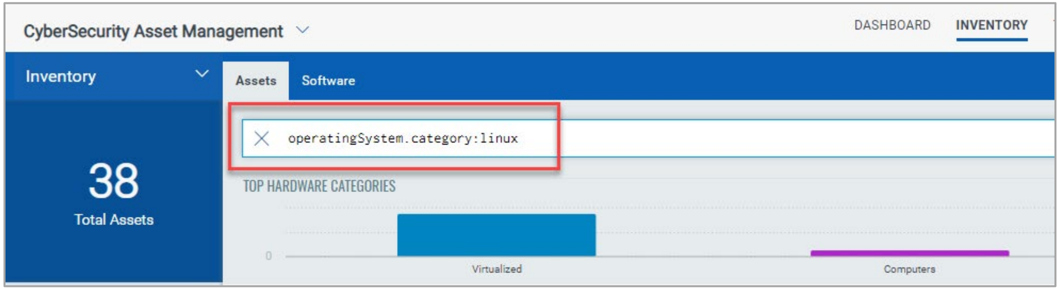
VMDR **Vulnerability Management, Detection, and Response**

Detect and Patch the PwnKit Vulnerability

Polkit is an application-level toolkit that controls system-wide privileges in Unix-like operating systems. Pwnkit (CVE-2021-4034) is a privilege corruption vulnerability in Polkit's pkexec SUID library. It allows an unprivileged process to communicate with a privileged process. Qualys recommends applying patches for this vulnerability immediately. If you are a Qualys customer, we recommend searching the vulnerability knowledgebase for CVE 2021-4034 to identify all the QIDs and assets vulnerable to this vulnerability.

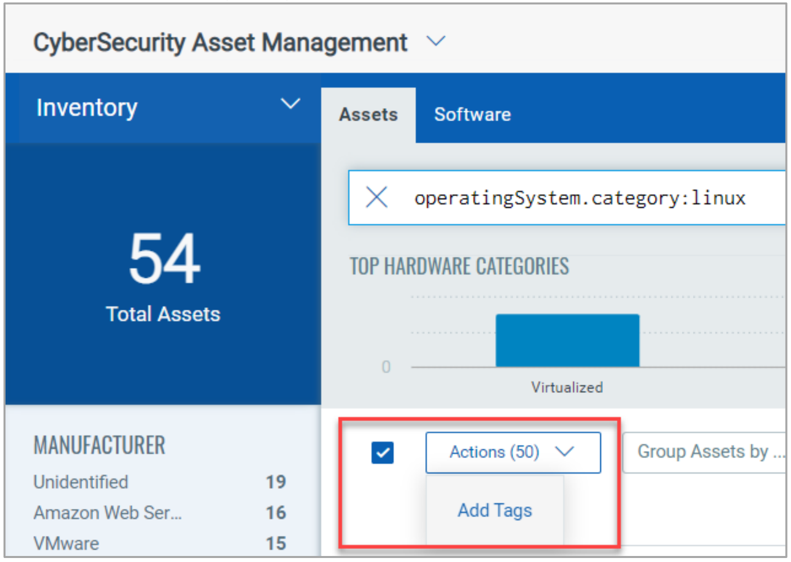
Perform the following steps to detect and patch the Pwnkit vulnerability:

1. In the **CyberSecurity Asset Management (CSAM)** module, click the **Inventory** tab.
2. In the **Assets** tab, enter the query **operatingSystem.category:linux**.



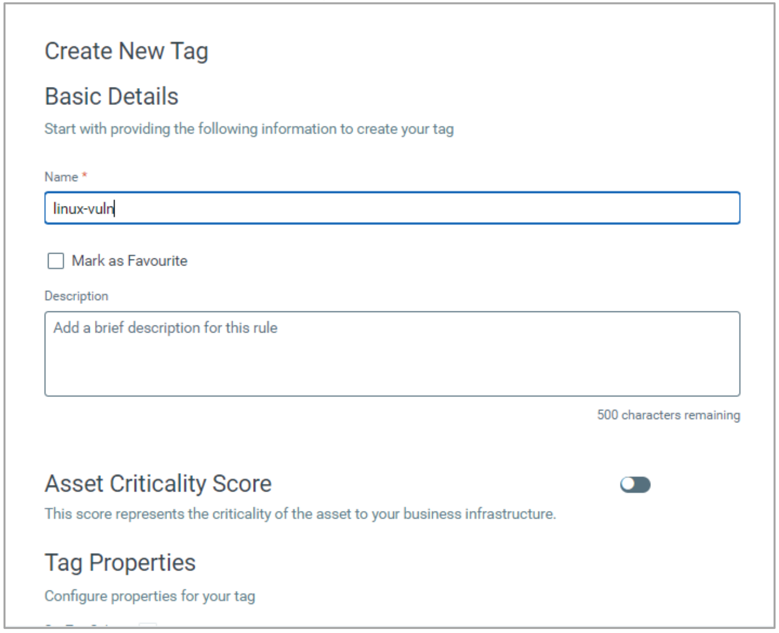
operatingSystem.category:linux

3. After the list gets generated, from the **Actions** drop-down menu, click **Add Tags**.



operatingSystem.category:linux

4. Click **Create New Tag** for the identified hosts.



Create New Tag

Basic Details

Start with providing the following information to create your tag

Name *

linux-vuln

□ Mark as Favourite

Description

Add a brief description for this rule

500 characters remaining

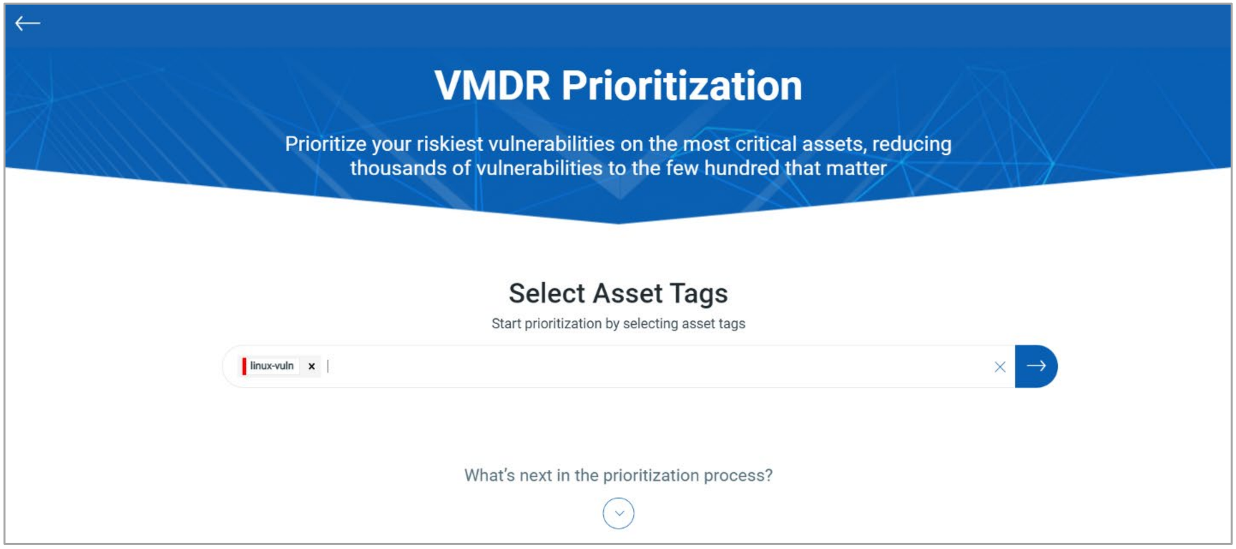
Asset Criticality Score

This score represents the criticality of the asset to your business infrastructure.

Tag Properties

Configure properties for your tag

5. In the **Vulnerability Management Detection and Response (VMDR)** module, click the **Prioritization** tab.
6. Click **Reports** > **Start Prioritizing**.



VMDR Prioritization

Prioritize your riskiest vulnerabilities on the most critical assets, reducing thousands of vulnerabilities to the few hundred that matter

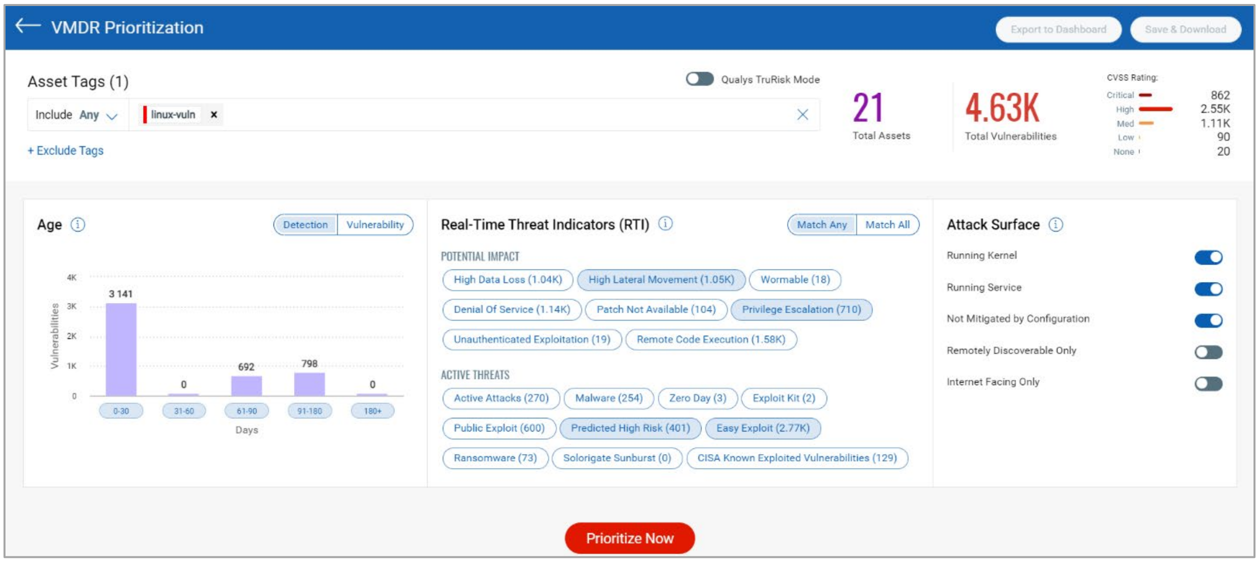
Select Asset Tags

Start prioritization by selecting asset tags

linux-vuln ×

What's next in the prioritization process?

7. Select the following **Real-Time Threat Indicators (RTI)**:
    - High Lateral Movement (Potential Impact)
    - Privilege Escalation (Potential Impact)
    - Predicted High Risk (Active Threats)
    - Easy Exploit (Active Threats)

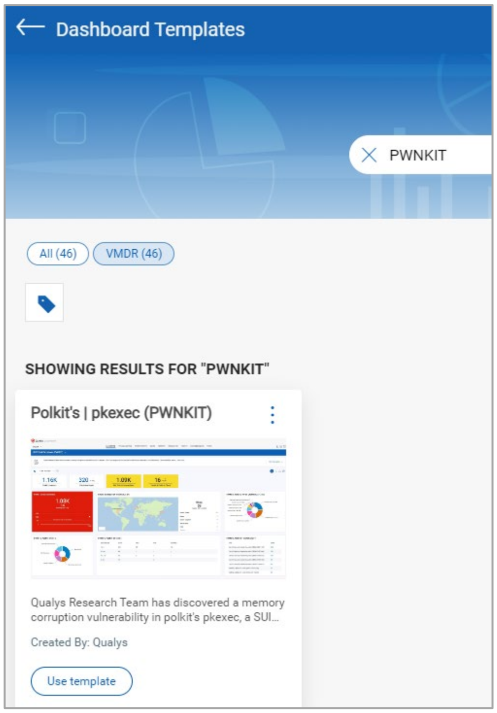


8. Click **Prioritize Now**.
9. Click **Patch Now** to apply the patch job once the vendors release the patches.

New PWNKIT Dashboard Template

With this release, we have introduced **PWNKIT** dashboard template. This template helps you to track the Polkit vulnerability, its impacted hosts and statuses along with overall management in real time. Perform the following steps to use the **PWNKIT** template:

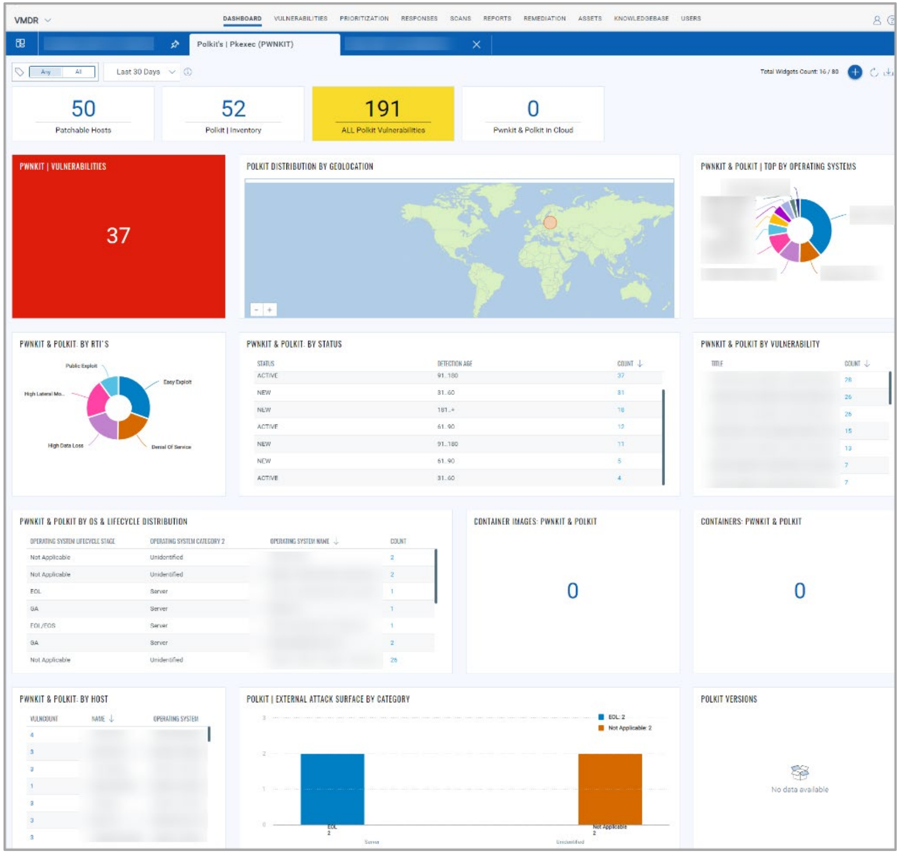
1. In the **VMDR** module, click
2. Select **Create New Dashboard**.
3. In the **Search for Dashboard Templates** search bar, type **PWNKIT**.
4. Click **Use Template**.



Qualys Research Team has discovered a memory corruption vulnerability in polkit's pkexec, a SUI...

Created By: Qualys

The **PWNKIT** template is displayed as follows:



PWNKIT & POLKIT: BY STATUS

STATUS	DETECTION AGE	COUNT ↓
ACTIVE	91..180	37
NEW	31..60	31
NEW	181..+	18
ACTIVE	61..90	12
NEW	91..180	11
NEW	61..90	5
ACTIVE	31..60	4

PWNKIT & POLKIT BY VULNERABILITY

TITLE	COUNT ↓
[redacted]	28
[redacted]	26
[redacted]	26
[redacted]	15
[redacted]	13
[redacted]	7
[redacted]	7

PWNKIT & POLKIT BY OS & LIFECYCLE DISTRIBUTION

OPERATING SYSTEM LIFECYCLE STAGE	OPERATING SYSTEM CATEGORY 2	OPERATING SYSTEM NAME ↓	COUNT
Not Applicable	Unidentified	[redacted]	2
Not Applicable	Unidentified	[redacted]	2
EOL	Server	[redacted]	1
GA	Server	[redacted]	1
EOL/EOS	Server	[redacted]	1
GA	Server	[redacted]	2
Not Applicable	Unidentified	[redacted]	26

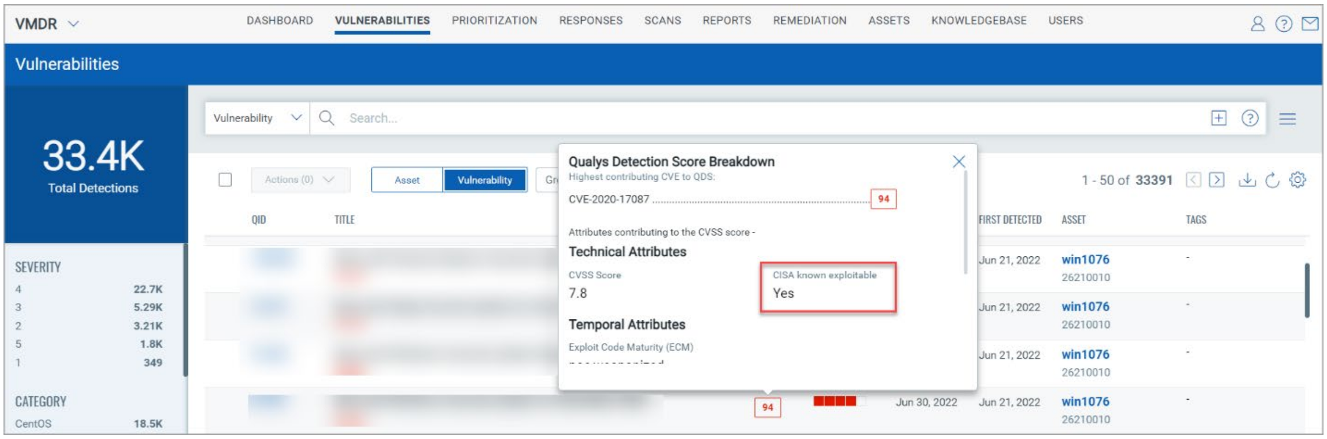
CONTAINER IMAGES: PWNKIT & POLKIT
0
CONTAINERS: PWNKIT & POLKIT
0

PWNKIT & POLKIT: BY HOST

VULNCOUNT	NAME ↓	OPERATING SYSTEM
4	[redacted]	[redacted]
3	[redacted]	[redacted]
3	[redacted]	[redacted]
1	[redacted]	[redacted]
3	[redacted]	[redacted]
3	[redacted]	[redacted]
3	[redacted]	[redacted]

CISA Vulns Renamed in Vulnerabilities Tab

In this release, we have renamed the CISA Vulns to **CISA known exploitable** in the **Vulnerabilities** tab. The CISA known exploitable is one of the contributing factors while calculating the Qualys Vulnerability Score (QVS).



SEVERITY

4	22.7K
3	5.29K
2	3.21K
5	1.8K
1	349

CATEGORY

CentOS	18.5K

Qualys Detection Score Breakdown

Highest contributing CVE to QDS:

CVE-2020-17087 94

Attributes contributing to the CVSS score -

Technical Attributes

CVSS Score: 7.8

CISA known exploitable: Yes

Temporal Attributes

Exploit Code Maturity (ECM)

FIRST DETECTED	ASSET	TAGS
Jun 21, 2022	win1076 26210010	-
Jun 21, 2022	win1076 26210010	-
Jun 21, 2022	win1076 26210010	-
Jun 21, 2022	win1076 26210010	-

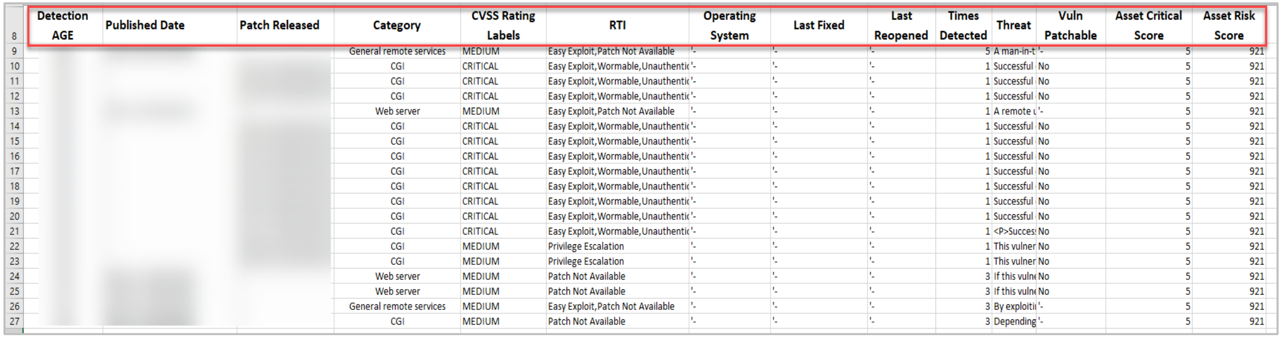
New Data Fields for Asset and Vulnerability Report

With this release, we have introduced new Asset, CVE, and QID data fields which are included when you download the Asset or Vulnerability Report. By default, the **Select All** checkbox is selected. You can uncheck the data fields you do not want in the Download report.

- Following are the new data fields added for **CVE** and **QID**:

  CVSS Rating Labels (only for CVE), QDS Severity (only for QID), KB Severity, Detection Age, Published Date, Patch Released, Category, RTI, Operating System, Last Fixed, Last Reopened, Times Detected, Threat, Vuln Patchable, Asset Critical Score, and Asset Risk Score.

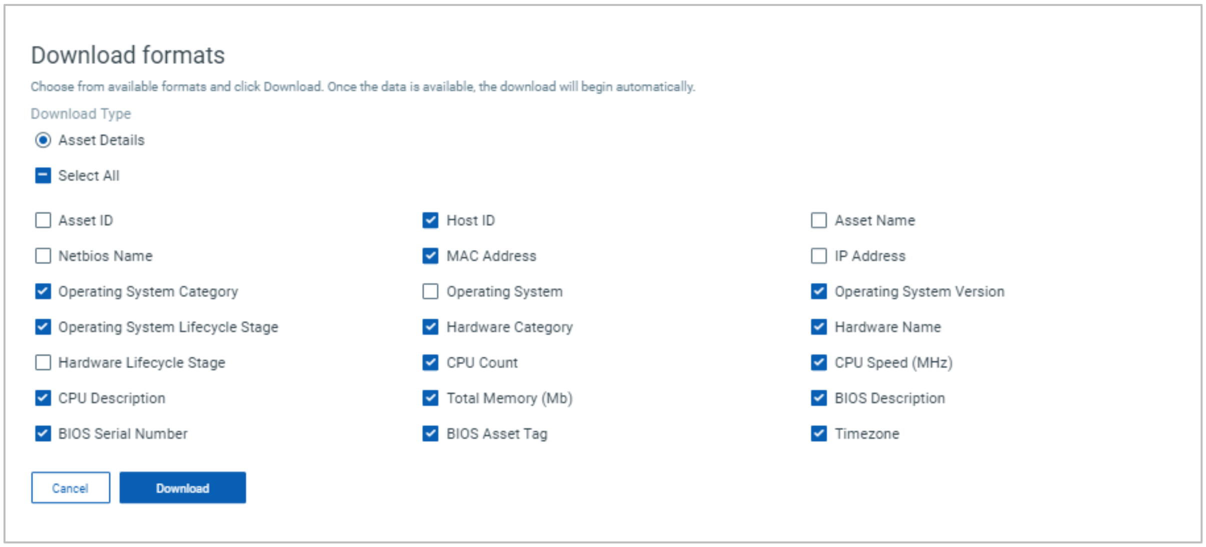
  The following screenshot is an example of the new CVE fields downloaded in a CSV format:



8	Detection AGE	Published Date	Patch Released	Category	CVSS Rating Labels	RTI	Operating System	Last Fixed	Last Reopened	Times Detected	Threat	Vuln Patchable	Asset Critical Score	Asset Risk Score
9	[redacted]	[redacted]		General remote services	MEDIUM	Easy Exploit,Patch Not Available	'-	'-	'-	5	A man-in-t	'-	5	921
10	[redacted]		[redacted]	CGI	CRITICAL	Easy Exploit,Wormable,Unauthentic	'-	'-	'-	1	Successful	No	5	921
11	[redacted]		[redacted]	CGI	CRITICAL	Easy Exploit,Wormable,Unauthentic	'-	'-	'-	1	Successful	No	5	921
12	[redacted]		[redacted]	CGI	CRITICAL	Easy Exploit,Wormable,Unauthentic	'-	'-	'-	1	Successful	No	5	921
13	[redacted]	[redacted]		Web server	MEDIUM	Easy Exploit,Patch Not Available	'-	'-	'-	1	A remote u	'-	5	921
14	[redacted]		[redacted]	CGI	CRITICAL	Easy Exploit,Wormable,Unauthentic	'-	'-	'-	1	Successful	No	5	921
15	[redacted]		[redacted]	CGI	CRITICAL	Easy Exploit,Wormable,Unauthentic	'-	'-	'-	1	Successful	No	5	921
16	[redacted]		[redacted]	CGI	CRITICAL	Easy Exploit,Wormable,Unauthentic	'-	'-	'-	1	Successful	No	5	921
17	[redacted]		[redacted]	CGI	CRITICAL	Easy Exploit,Wormable,Unauthentic	'-	'-	'-	1	Successful	No	5	921
18	[redacted]		[redacted]	CGI	CRITICAL	Easy Exploit,Wormable,Unauthentic	'-	'-	'-	1	Successful	No	5	921
19	[redacted]		[redacted]	CGI	CRITICAL	Easy Exploit,Wormable,Unauthentic	'-	'-	'-	1	Successful	No	5	921
20	[redacted]		[redacted]	CGI	CRITICAL	Easy Exploit,Wormable,Unauthentic	'-	'-	'-	1	Successful	No	5	921
21	[redacted]		[redacted]	CGI	CRITICAL	Easy Exploit,Wormable,Unauthentic	'-	'-	'-	1	<P>Succes	No	5	921
22	[redacted]		[redacted]	CGI	MEDIUM	Privilege Escalation	'-	'-	'-	1	This vulner	No	5	921
23	[redacted]		[redacted]	CGI	MEDIUM	Privilege Escalation	'-	'-	'-	1	This vulner	No	5	921
24	[redacted]	[redacted]		Web server	MEDIUM	Patch Not Available	'-	'-	'-	3	If this vulne	No	5	921
25	[redacted]	[redacted]		Web server	MEDIUM	Patch Not Available	'-	'-	'-	3	If this vulne	No	5	921
26	[redacted]	[redacted]		General remote services	MEDIUM	Easy Exploit,Patch Not Available	'-	'-	'-	3	By exploitii	'-	5	921
27	[redacted]	[redacted]		CGI	MEDIUM	Patch Not Available	'-	'-	'-	3	Depending	'-	5	921

- Following are the new data fields added for **Asset**:

  Host Id, Mac Address, Operating System Category, Operating System Version, Operating System Lifecycle Stage, Hardware Category, Hardware Name, Hardware Lifecycle Stage, CPU Count, CPU Speed (mhz), CPU Description, Total Memory (mb), Bios Description, Bios Serial Number, Bios Asset Tag, Time Zone, Last System Boot, Inventory Source, Agent Id, Architecture, Hardware Uuid



Download formats

Choose from available formats and click Download. Once the data is available, the download will begin automatically.

Download Type

● Asset Details

▣ Select All

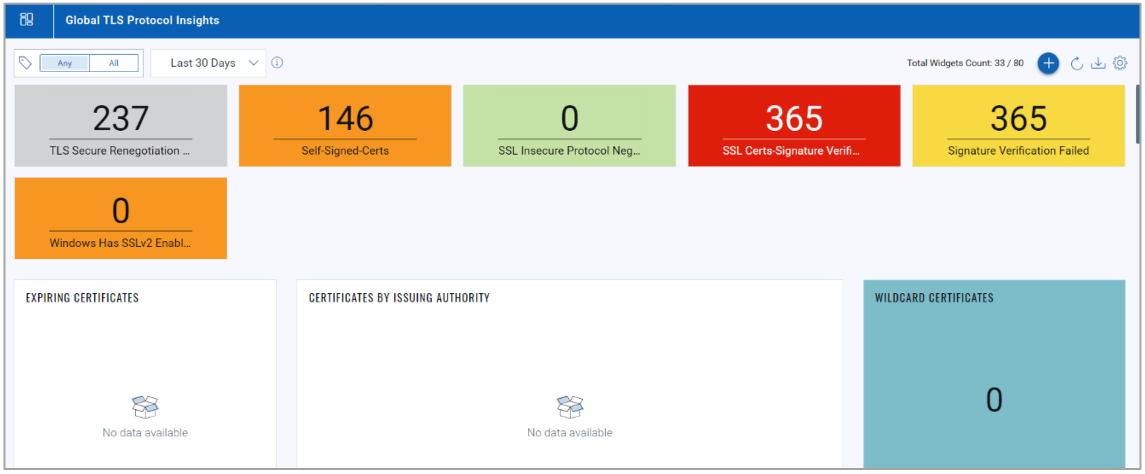
☐ Asset ID	☑ Host ID	☐ Asset Name
☐ Netbios Name	☑ MAC Address	☐ IP Address
☑ Operating System Category	☐ Operating System	☑ Operating System Version
☑ Operating System Lifecycle Stage	☑ Hardware Category	☑ Hardware Name
☐ Hardware Lifecycle Stage	☑ CPU Count	☑ CPU Speed (MHz)
☑ CPU Description	☑ Total Memory (Mb)	☑ BIOS Description
☑ BIOS Serial Number	☑ BIOS Asset Tag	☑ Timezone

New Global TLS Protocol Insights Dashboard Template

With this release, we have introduced a new dashboard template **Global TLS Protocol Insights**. The template reports on All Certificates and TLS Vulnerability detections across your organization. Perform the following steps to use the template:

1. In the **VMDR** module, click ⚙
2. Select **Create New Dashboard**
3. In the **Search for Dashboard Templates** search bar, type **Global TLS Protocol Insights**
4. Click **Use Template**

The **Global TLS Protocol Insights** template is displayed.


Global TLS Protocol Insights
Any
All
Last 30 Days
Total Widgets Count: 33 / 80
237
TLS Secure Renegotiation ...
146
Self-Signed-Certs
0
SSL Insecure Protocol Neg...
365
SSL Certs-Signature Verifi...
365
Signature Verification Failed
0
Windows Has SSLv2 Enabl...
EXPIRING CERTIFICATES
No data available
CERTIFICATES BY ISSUING AUTHORITY
No data available
WILDCARD CERTIFICATES
0

Updated Tokens for VMDR

- **vulnerabilities.vulnerability.cvss3_1Info.baseScore:** We have updated the base score with the CVSS version 3.1 for the VM application.
- **vulnerabilities.vulnerability.cvss3_1Info.temporalScore:** We have updated the temporal score with the CVSS version 3.1 for the VM application.

Issues Addressed

VM

Vulnerability Management

- We have fixed an issue where the column names of the **Table** widget output would appear misaligned.
- We have fixed an issue where the **MTTR** value in the **Average** widget was mismatched with the query provided.
- We have fixed an issue where the **Ratio** widget did not generate the trendline.
- The issue where double underscores were observed in the **Detection Summary** of the **Vulnerability Details** tab is now resolved.
- Previously, when you downloaded a CSV report from **VMDR Vulnerabilities** tab, the formatting would get disrupted due to the cell character limitation in Microsoft Excel. With this release, we have introduced a workaround for this issue. If you now download a CSV report with more than 30000 characters in a single cell of the **Results** column, a new column(s) named Result is added in such cases. These new columns are named **Result_1**, **Result_2**, and so on.
- The widgets with trending enabled observed a sudden spike in the trend if they used the following tokens in the search query.
  - operatingSystem
  - operatingSystem.name
  - software.name
  - software.version

  To resolve this issue, we have now introduced a new flag that allows you to choose seamless data sync between **CyberSecurity Asset Management (CSAM)** and **Vulnerability Management Detection and Response (VMDR)** modules. By default, the flag is set as false.

  You can enable the CSAM data sync feature by contacting Qualys Support. Enabling this feature/flag may lead to spikes in widgets that use any of the above tokens and have trending enabled.
- We fixed an issue where VM scans were not getting processed due to duplicate key/unique constraint exception while processing the network interface of an asset, and asset processing was dropped. To fix this, we have now dropped a unique constraint on asset_host_addr, that is, ASSET_HOST_ADDR_UK1.
- We fixed an issue where no Trending data was displayed for some CSAM widgets. To resolve this issue, we have now added the following search tokens in Trending data:
  - sensors.lastVmScanDateAgent
  - sensors.lastVmScanDateScanner
- We fixed an issue where the user could not update the parent tag of Asset Group using APIs. The APIs are fixed in a way that now the user can update the parent tag of Asset Group.

AV AssetView

- The widgets with trending enabled observed a sudden spike in the trend if they used the following tokens in the search query.
  - operatingSystem
  - operatingSystem.name
  - software.name
  - software.version

  To resolve this issue, we have now introduced a new flag that allows you to choose seamless data sync between **CyberSecurity Asset Management (CSAM)** and **AssetView** modules. By default, the flag is set as false.

  We would recommend you to keep this flag as disabled and use the search queries in the **CyberSecurity Asset Management (CSAM)** module for resource inventory.

CA Cloud Agent

- We have fixed an issue where a user with the 'READER' role was not able to add, remove or create an asset tag in the **Agents** and **Configuration Profiles** tab.

- The user was facing issues while activating Cloud Agent for some modules in bulk using APIs when the license count was insufficient. We have fixed this issue.

WAF Web Application Firewall

- We have fixed an issue where an error occurred while updating the WAF cluster owner in a case where the earlier owner has left the organization. Now, all users under the same subscription can switch ownership of all the resources.