Qualys.

Qualys Cloud Platform v3.x

Release Notes

Version 3.5
February 24, 2021 (updated on March 15, 2021)

Here's what's new in Qualys Cloud Suite 3.5!

VMDR Vulnerability Management Detection and Response

New Fields Added to "Group By" Search Results for Vulnerabilities
New Search Tokens Introduced

UD Unified Dashboard

New Templates for Dashboards
None Option Supported for Group By in Widget Builder
New Data Points for Simple Table Widget
Enhanced Support for Dashboard Description
Dashboards Downloadable in PDF Format
Manage Dashboard and Widget Templates
Multi-Grouped Table Widgets: Status and Type Detected Group By Filters Enhanced

WAS Web Application Scanning

Support for CVSS V3 Scoring System for Vulnerabilities
Assignment of System Tags and Dynamic Tags Not Supported from WAS UI

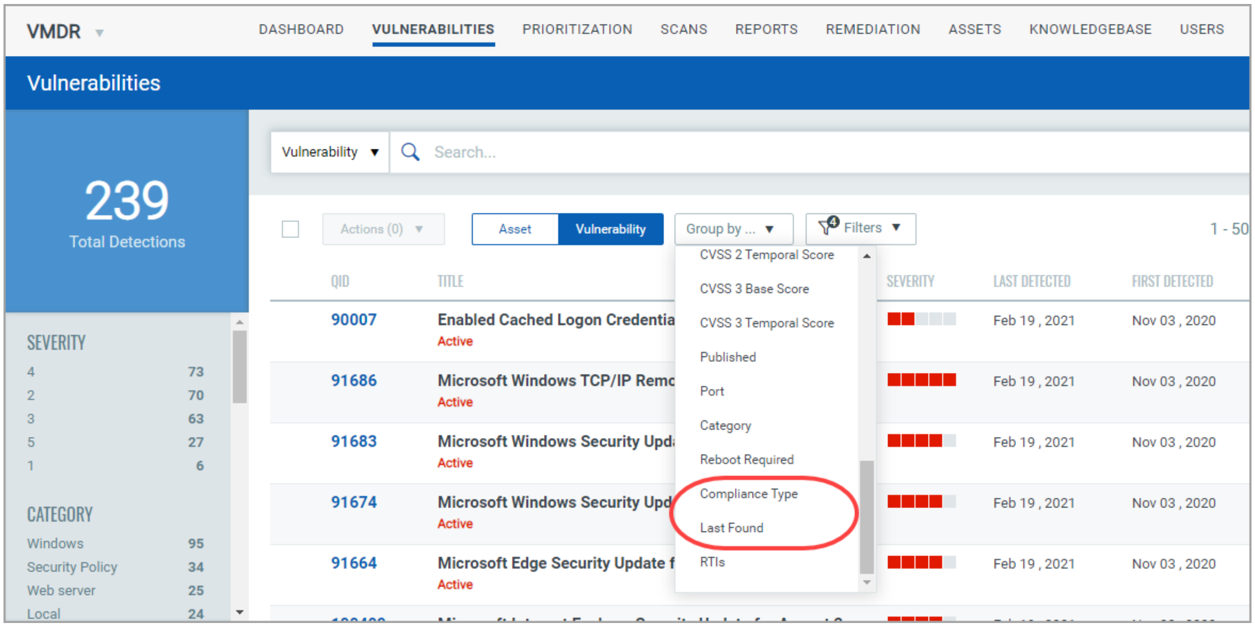
Administration Module

Global Dashboard Permissions

Qualys Cloud Platform 3.5 brings you many more Improvements and updates! Learn more

New Fields Added to “Group By” Search Results for Vulnerabilities

We have now made following additions to “Group by” to simplify your seach results for vulnerabilities.
- Compliance Type: You could group vulnerabilities depending on various complaince types such as COBIT, HIPAA, GLBA, SOX, PC, and so on.
- Last Found: We provide pre-defined range of days for vulnerabilities that were discovered recently. The range categories are like 0 – 3, 4 – 7, 8 – 15, 16 – 30, 31 – 60, 61 – 90, 91 – 180, 181 – 365, 366 ..+ and so on.



SEVERITY	
4	73
2	70
3	63
5	27
1	6

CATEGORY	
Windows	95
Security Policy	34
Web server	25
Local	24

QID	TITLE	SEVERITY	LAST DETECTED	FIRST DETECTED
90007	Enabled Cached Logon Credentia Active	🟥🟥⬜⬜⬜	Feb 19 , 2021	Nov 03 , 2020
91686	Microsoft Windows TCP/IP Remc Active	🟥🟥🟥🟥🟥	Feb 19 , 2021	Nov 03 , 2020
91683	Microsoft Windows Security Upd Active	🟥🟥🟥🟥⬜	Feb 19 , 2021	Nov 03 , 2020
91674	Microsoft Windows Security Upd Active	🟥🟥🟥🟥⬜	Feb 19 , 2021	Nov 03 , 2020
91664	Microsoft Edge Security Update f Active	🟥🟥🟥🟥⬜	Feb 19 , 2021	Nov 03 , 2020

New Search Tokens Introduced

We have introduced two new search tokens to enhance your search results for assets:
- qid
- connectedFrom

UD Unified Dashboard

New Templates for Dashboards

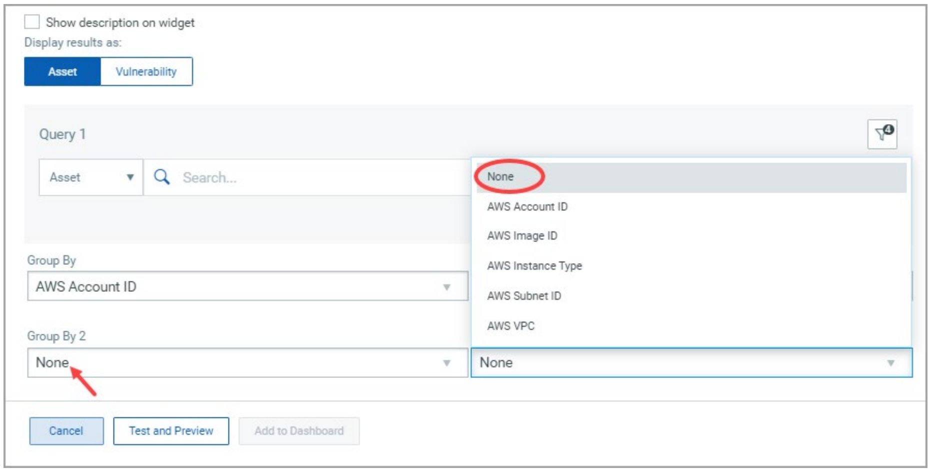
We have now enhanced our template library with addition of several new templates. You can use these pre-defined template dashboard to have a single-pane-of-glass view on the dashboard for assets with specific areas of concern.

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

- **FritzFrog Malware QID1052**: Enables detection of FritzFrog with Inventory Data.
- **Zoom Client Multiple Vulns (Windows)**: Supports Qualys Blog Post about Secure Remote Endpoints from Vulnerabilities in Video Conferencing & Productivity Applications such as Zoom, specifically for Windows endpoints.
- **Zoom Client Multiple Vulns (MAC)**: Supports Qualys Blog Post about Secure Remote Endpoints from Vulnerabilities in Video Conferencing & Productivity Applications such as Zoom, specifically for MAC endpoints.
- **PHP RCE Vulnerability | CVE-2019-11043**: Provides PHP Remote Code Execution Vulnerability (CVE-2019-11043).
- **Open Confirmed Within 6M | Adobe**: Provides view of all your Adobe-related inventory and Adobe product-related vulnerabilities.
- **Oracle Patch Review**: Provides view of all your Oracle-related inventory and Oracle product-related vulnerabilities.
- **Oracle Weblogic Server | CVE-2020-2883**: Provides view of all Oracle Weblogic Server vulnerabilities.
- **ZeroLogon | CVE-2020-1472**: Provides vulnerabilities related to CVE-2020-1472, which received a maximum severity rating score of 10.0 on CVSS v3 Scoring system.
- **Palo Alto Networks Vuln View**: Provides Palo Alto Network devices related vulnerabilities.
- **NSA's Top 25 Vulnerabilities from China**: Lists the top 25 publicly known vulnerabilities known to be leveraged by cyber actors from Chinese state-sponsored malicious cyber actors group: NSA's Top 25 Vulnerabilities from China.
- **Citrix ADC and Gateway RCE CVE-2019-19781**: Lists the vulnerabilities related to CVE-2019-19781 – a remote code execution vulnerability in Citrix Application Delivery Controller (ADC) and Citrix Gateway products.
- **EDR-Windows MITRE ATT&CK**: Comprises several widgets specific to the techniques included in the MITRE ATT&CK framework, which populates as soon as any of your monitored assets fall prey to malicious activities.
- **FIM Windows MITRE ATT&CK**: Comprises several widgets specific to the techniques included in the MITRE ATT&CK framework, which populates as soon as any of your monitored Windows assets falls prey to malicious activities.
- **FIM LINUX MITRE ATT&CK:** Comprises several widgets specific to the techniques included in the MITRE ATT&CK framework, which populates as soon as any of your monitored Linux assets falls prey to malicious activities.
- **FIM Linux NIST Special Publication 800-53**: Comprises several widgets specific to the Security and Privacy Controls for Federal Information Systems and Organizations, which populate as soon as any of your monitored assets fall prey to malicious activities.

None Option Supported for Group By in Widget Builder

We have enhanced the Group By options in the widget builder to simplify the widget building process. We now include “None” in the Group By fields of the Multi-Grouped table widget. As a result, swapping group by fields is now easier with usage of None in the drop-down options.



□ Show description on widget

Group By: AWS Account ID

Group By 2: None | None

New Data Points for Simple Table Widget

We have now added support for three new data points that can be included as a column when you build a simple table widget.

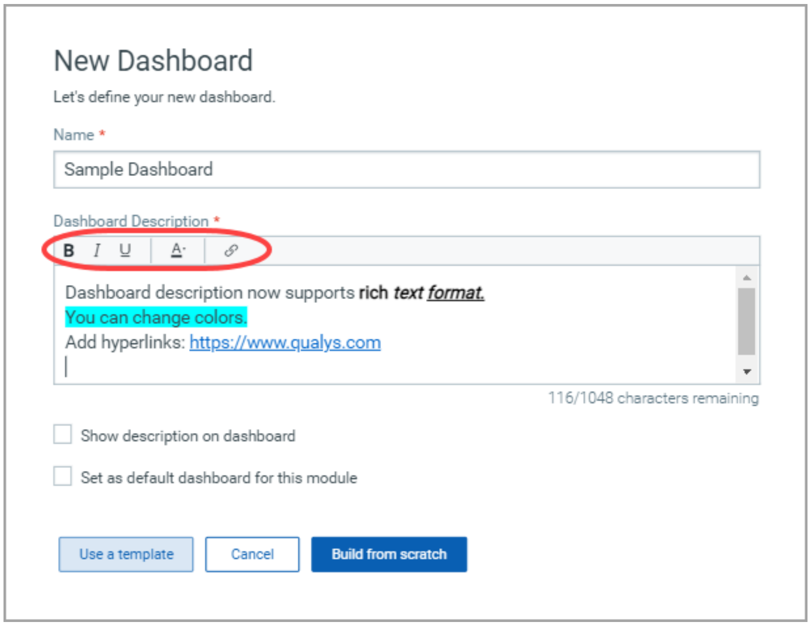
The new data points that are now supported for Simple table widget are:

- NetBios Name
- Host Name
- IP Address

Enhanced Support for Dashboard Description

We have now added rich text format support for dashboard descriptions.

Now, when you create a dashboard you, the description field for dashboards supports rich text formatting. You can In addition to bold, italics, and underline formatting, you can also include hyperlinks to other blogs, policies, posts or internet articles in the dashboard description.



New Dashboard

Let's define your new dashboard.

Name *: Sample Dashboard

Dashboard Description *:

Dashboard description now supports **rich *text* _format._**
You can change colors.
Add hyperlinks: https://www.qualys.com

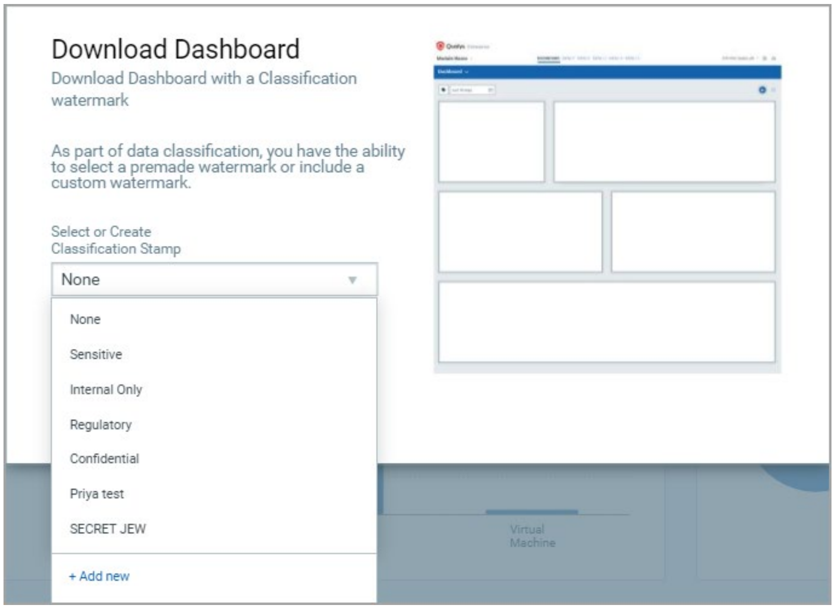
□ Show description on dashboard

□ Set as default dashboard for this module

Dashboards Downloadable in PDF Format

You can now download dashboard in PDF report format. You could also add pre-defined or custom stamp classification as header to the PDF report.

On Dashboards tab, select the dashboard to be downloaded and click the ⤓ icon to download dashbord in PDF report format.



Download Dashboard

Download Dashboard with a Classification watermark

As part of data classification, you have the ability to select a premade watermark or include a custom watermark.

Select or Create Classification Stamp

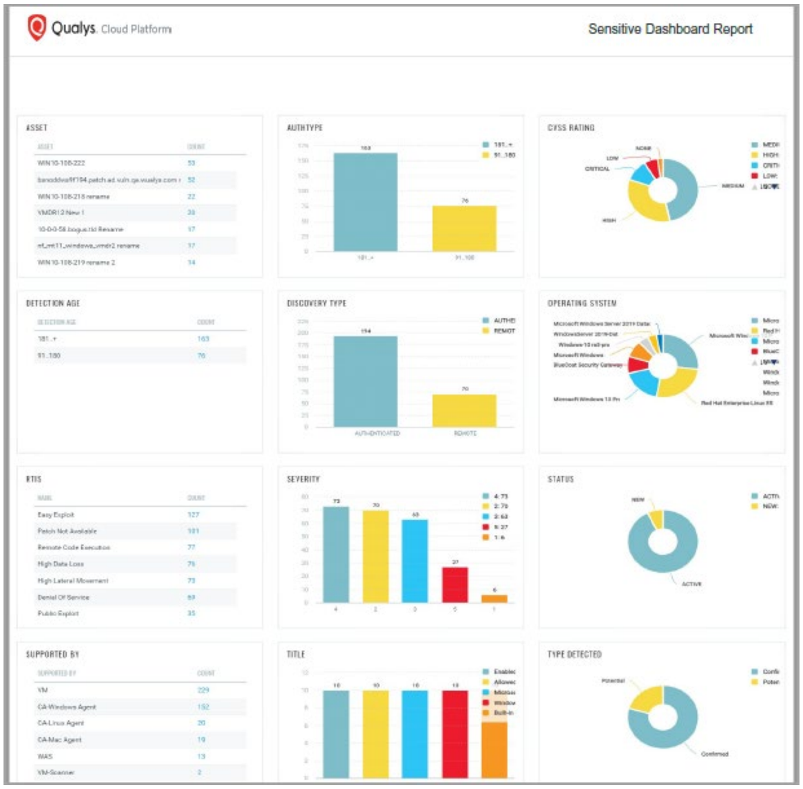
None ▾

Select pre-defined or custom stamp classification (optional) to be added as header to the PDF report format. Alternately, click Add new to create custom header text, and then click **Download Dashboard**.

A new tab is opened when the PDF report of the dashboard is being generated. Once the PDF is downloaded, the new tab automatically closes.

Note: The Dashboard description is not included in the PDF report.

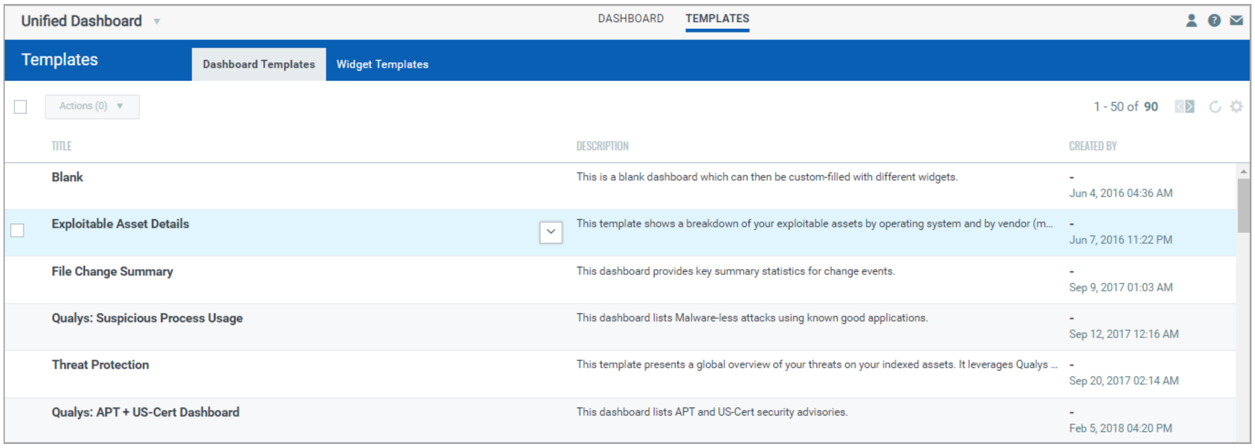
Dashboard in PDF Report format



Manage Dashboard and Widget Templates

We have now added dedicated tab for dashboard and widget templates. You can now view, edit, delete and manage all user-defined widgets and dashboards at one place. You can also delete bulk templates at one go.

In the Unified Dashboard app, go to **Templates** tab.



TITLE	DESCRIPTION	CREATED BY
Blank	This is a blank dashboard which can then be custom-filled with different widgets.	- Jun 4, 2016 04:36 AM
Exploitable Asset Details	This template shows a breakdown of your exploitable assets by operating system and by vendor (m...	- Jun 7, 2016 11:22 PM
File Change Summary	This dashboard provides key summary statistics for change events.	- Sep 9, 2017 01:03 AM
Qualys: Suspicious Process Usage	This dashboard lists Malware-less attacks using known good applications.	- Sep 12, 2017 12:16 AM
Threat Protection	This template presents a global overview of your threats on your indexed assets. It leverages Qualys ...	- Sep 20, 2017 02:14 AM
Qualys: APT + US-Cert Dashboard	This dashboard lists APT and US-Cert security advisories.	- Feb 5, 2018 04:20 PM

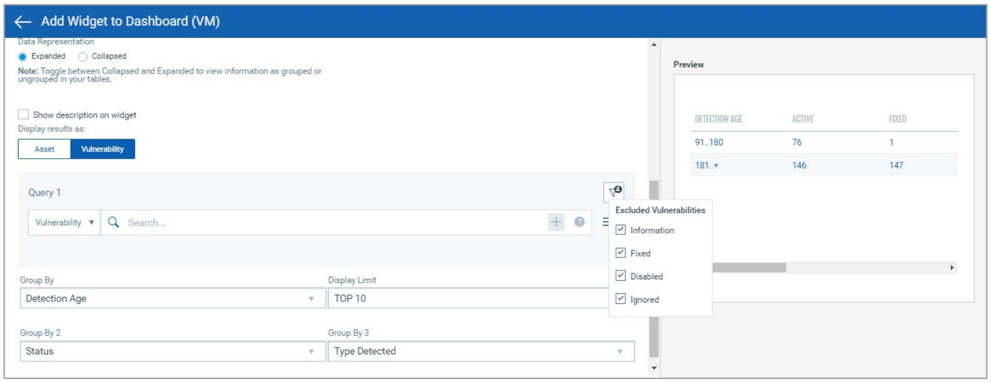
The Templates tab includes two sub tabs:
- **Dashboard Templates**: Lists all the user-defined or edited dashboard templates.
- **Widget Templates**: Lists all the user-defined or edited widget templates.

Note: You can take actions on the templates that you created using the quick actions menu. You cannot edit or delete System templates.

Multi-Grouped Table Widgets: Status and Type Detected Group By Filters Enhanced

We have now enhanced the implementation of Group By Filters for Status and Type detected in the multi-grouped table widget builder.

If you choose **Status** as one of the Group By fields, the **Excluded Vulnerabilities** filter is not applicable to the **Fixed** status column in the multi-grouped table.
For example, let us build a multi-grouped table with Expanded data representation. The table data is grouped by Detection Age, Status, and Type Detected. The table preview now displays the Fixed column that includes the count of Fixed vulnerabilities (ignoring Fixed as excluded vulnerabilities.



Data Representation

● Expanded ○ Collapsed

Note: Toggle between Collapsed and Expanded to view information as grouped or ungrouped in your tables.

□ Show description on widget

Display results as: Vulnerability

Query 1

Vulnerability

Excluded Vulnerabilities

☑ Information

☑ Fixed

☑ Disabled

☑ Ignored

Group By: Detection Age

Display Limit: TOP 10

Group By 2: Status

Group By 3: Type Detected

DETECTION AGE	ACTIVE	FIXED
91..180	76	1
181..+	146	147

Similarly, if you choose **Type Detected** as one of the Group By fields, the **Excluded Vulnerabilities** filter is not applicable to the **Information** column in the table.

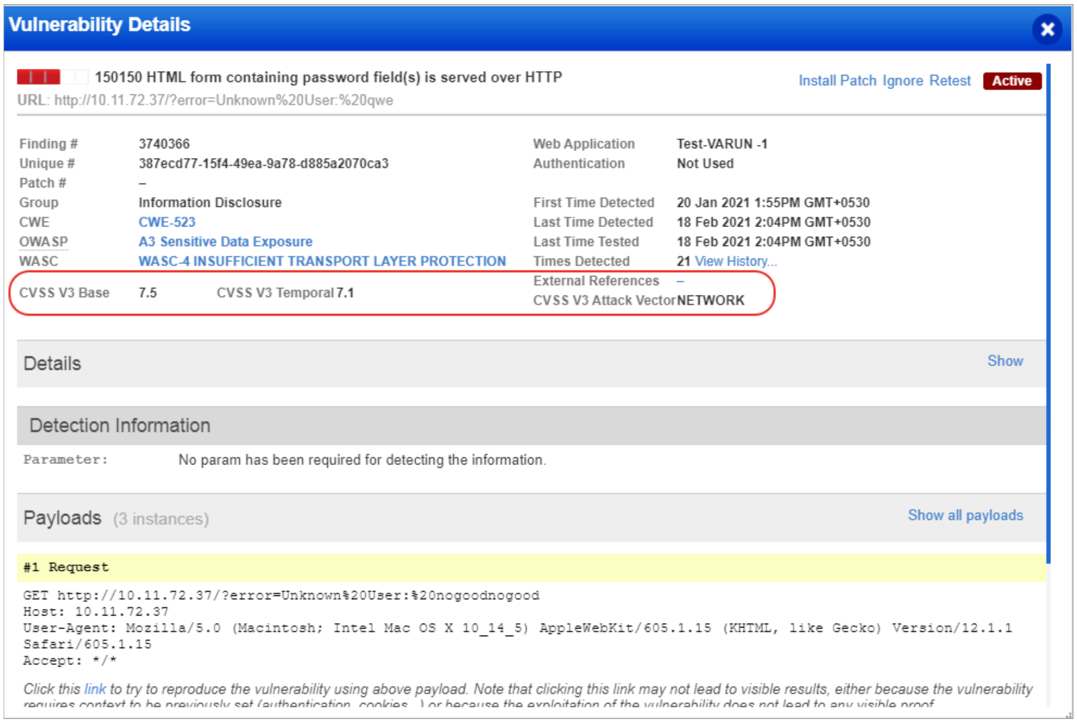
Support for CVSS V3 Scoring System for Vulnerabilities

With this release, we are supporting Common Vulnerability Scoring System CVSS V3 scoring system for Vulnerability and Sensitive Content QID types. We do not show CVSS V3 information for Information Gathered (IG) QID types. With the migration of CVSS scoring system to V3, you will now see the CVSS V3 information on all places where we used to show the CVSS V3 information. The information will include: CVSS V3 Base Score, CVSS V3 Temporal Score and CVSS V3 Attack Vector. For QIDs in KnowledgeBase, we show the CVSS V3 Base Score, CVSS V3 Temporal Score, and CVSS Vector String. CVSS Vector String is a combination of CVSS V3 metrics and their values as assigned to the vulnerability.

You will see this information in the Scan report, Web app report, Vulnerability details for findings from the Detections, for QIDs in KnowledgeBase. You can add CVSS V3 attributes in the search criteria while creating Dynamic Search List.

Note that reports in the XML, CSV, and CSV v2 formats show both CVSS V2 and CVSS V3 information. Reports in HTML and PDF formats show only CVSS v3 information.

Vulnerability Details from Detections List



Vulnerability Details

150150 HTML form containing password field(s) is served over HTTP

URL: http://10.11.72.37/?error=Unknown%20User:%20qwe

Finding #	3740366	Web Application	Test-VARUN -1
Unique #	387ecd77-15f4-49ea-9a78-d885a2070ca3	Authentication	Not Used
Patch #	–		
Group	Information Disclosure	First Time Detected	20 Jan 2021 1:55PM GMT+0530
CWE	CWE-523	Last Time Detected	18 Feb 2021 2:04PM GMT+0530
OWASP	A3 Sensitive Data Exposure	Last Time Tested	18 Feb 2021 2:04PM GMT+0530
WASC	WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION	Times Detected	21 View History...
		External References	–
CVSS V3 Base	7.5 CVSS V3 Temporal 7.1	CVSS V3 Attack Vector	NETWORK

Detection Information

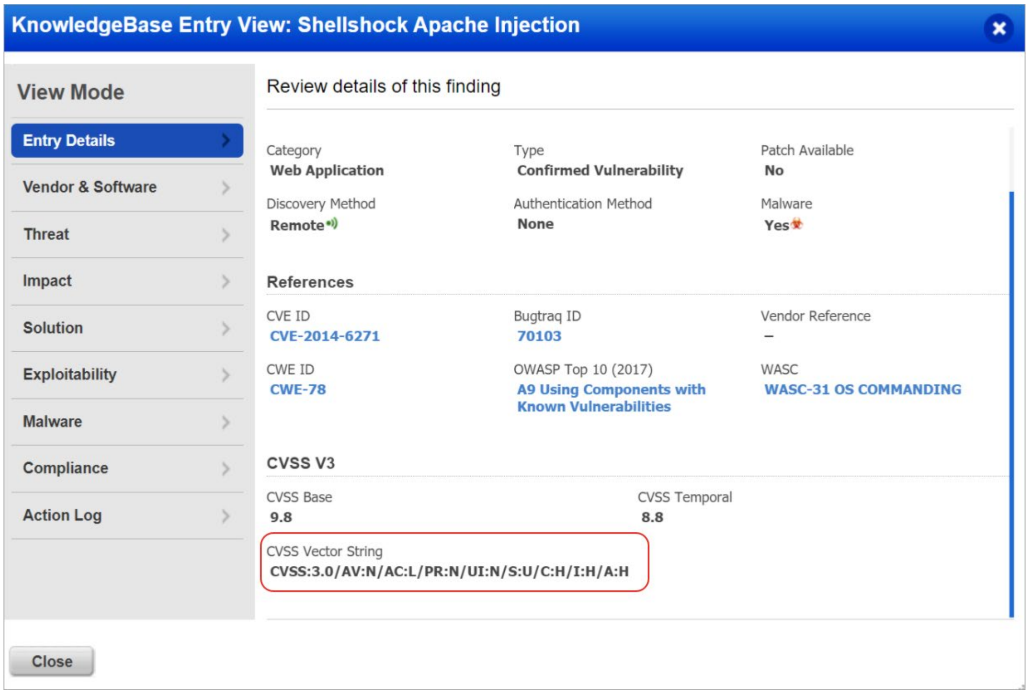
Parameter: No param has been required for detecting the information.

```
#1 Request

GET http://10.11.72.37/?error=Unknown%20User:%20nogoodnogood
Host: 10.11.72.37
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1
Safari/605.1.15
Accept: */*
```

Click this link to try to reproduce the vulnerability using above payload. Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies, ...) or because the exploitation of the vulnerability does not lead to any visible proof

KnowledgeBase QID Entry



KnowledgeBase Entry View: Shellshock Apache Injection

Review details of this finding

Category Web Application	Type Confirmed Vulnerability	Patch Available No
Discovery Method Remote	Authentication Method None	Malware Yes

References

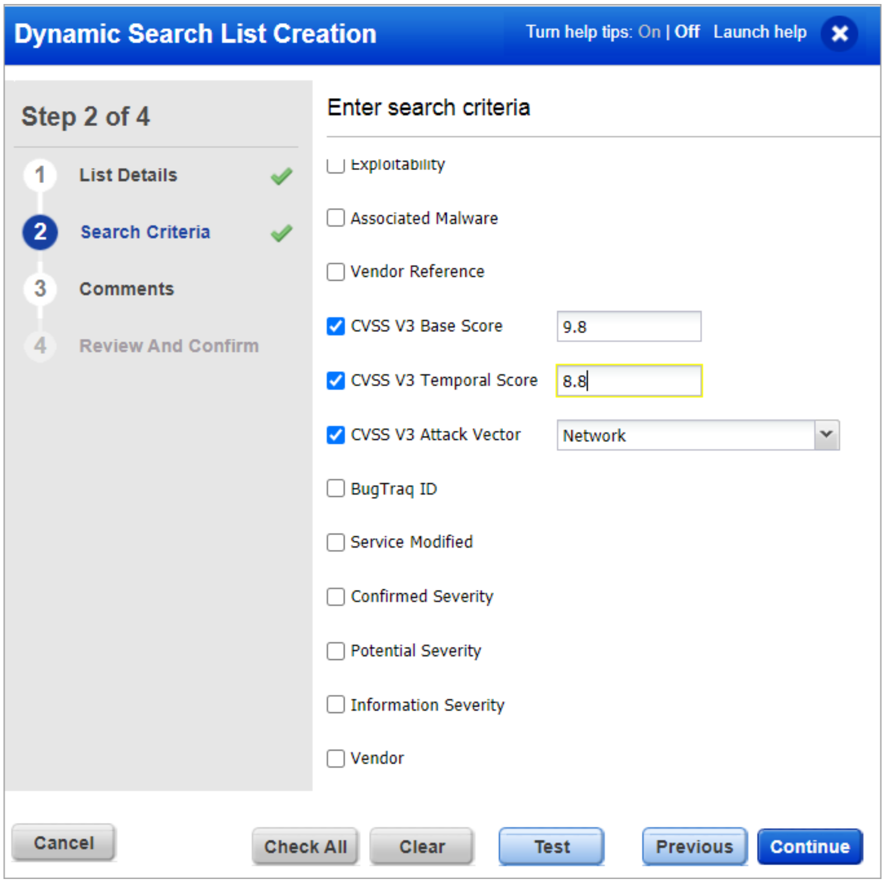
CVE ID CVE-2014-6271	Bugtraq ID 70103	Vendor Reference –
CWE ID CWE-78	OWASP Top 10 (2017) A9 Using Components with Known Vulnerabilities	WASC WASC-31 OS COMMANDING

CVSS V3

CVSS Base 9.8	CVSS Temporal 8.8

CVSS Vector String
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Dynamic Search List Criteria



Dynamic Search List Creation

Enter search criteria

□ Exploitability

□ Associated Malware

□ Vendor Reference

☑ CVSS V3 Base Score 9.8

☑ CVSS V3 Temporal Score 8.8

☑ CVSS V3 Attack Vector Network

□ BugTraq ID

□ Service Modified

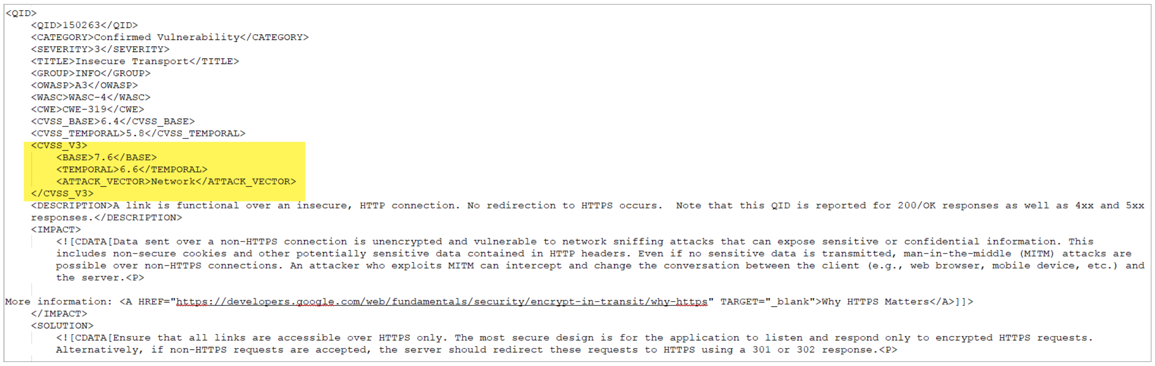
□ Confirmed Severity

□ Potential Severity

□ Information Severity

□ Vendor

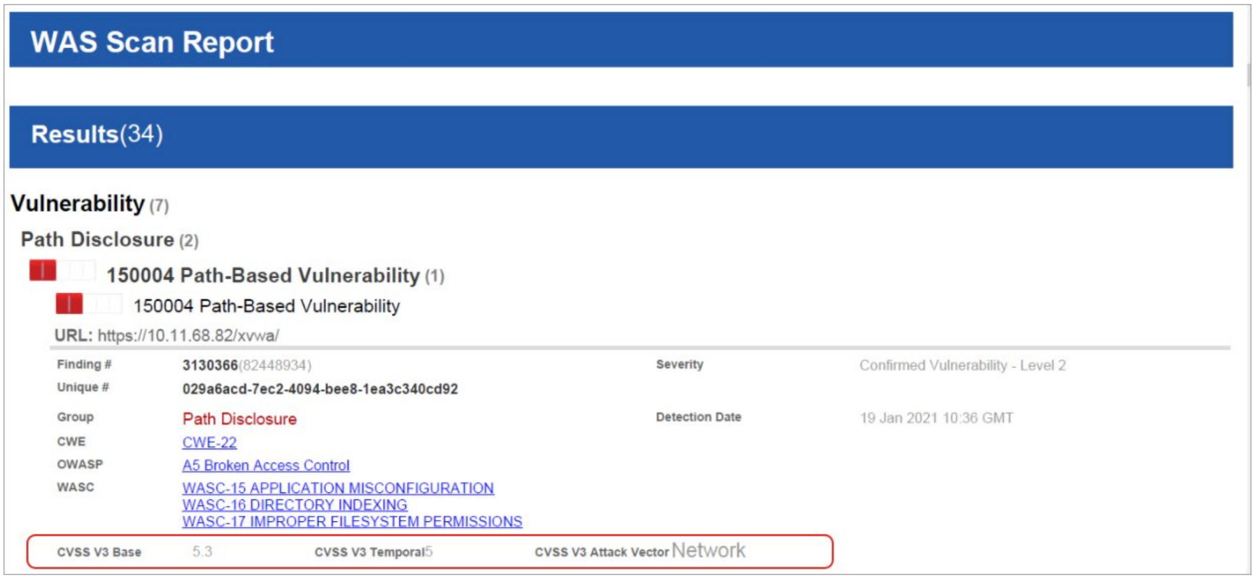
Web Application Report in XML format



```
<QID>
    <QID>150263</QID>
    <CATEGORY>Confirmed Vulnerability</CATEGORY>
    <SEVERITY>3</SEVERITY>
    <TITLE>Insecure Transport</TITLE>
    <GROUP>INFO</GROUP>
    <OWASP>A3</OWASP>
    <WASC>WASC-4</WASC>
    <CWE>CWE-319</CWE>
    <CVSS_BASE>6.4</CVSS_BASE>
    <CVSS_TEMPORAL>5.8</CVSS_TEMPORAL>
    <CVSS_V3>
        <BASE>7.6</BASE>
        <TEMPORAL>6.6</TEMPORAL>
        <ATTACK_VECTOR>Network</ATTACK_VECTOR>
    </CVSS_V3>
    <DESCRIPTION>A link is functional over an insecure, HTTP connection. No redirection to HTTPS occurs.  Note that this QID is reported for 200/OK responses as well as 4xx and 5xx
    responses.</DESCRIPTION>
    <IMPACT>
        <![CDATA[Data sent over a non-HTTPS connection is unencrypted and vulnerable to network sniffing attacks that can expose sensitive or confidential information. This
        includes non-secure cookies and other potentially sensitive data contained in HTTP headers. Even if no sensitive data is transmitted, man-in-the-middle (MITM) attacks are
        possible over non-HTTPS connections. An attacker who exploits MITM can intercept and change the conversation between the client (e.g., web browser, mobile device, etc.) and
        the server.<P>

More information: <A HREF="https://developers.google.com/web/fundamentals/security/encrypt-in-transit/why-https" TARGET="_blank">Why HTTPS Matters</A>]]>
    </IMPACT>
    <SOLUTION>
        <![CDATA[Ensure that all links are accessible over HTTPS only. The most secure design is for the application to listen and respond only to encrypted HTTPS requests.
        Alternatively, if non-HTTPS requests are accepted, the server should redirect these requests to HTTPS using a 301 or 302 response.<P>
```

Scan Report in PDF format



WAS Scan Report

Results(34)

Vulnerability (7)

Path Disclosure (2)

150004 Path-Based Vulnerability (1)

150004 Path-Based Vulnerability

URL: https://10.11.68.82/xvwa/

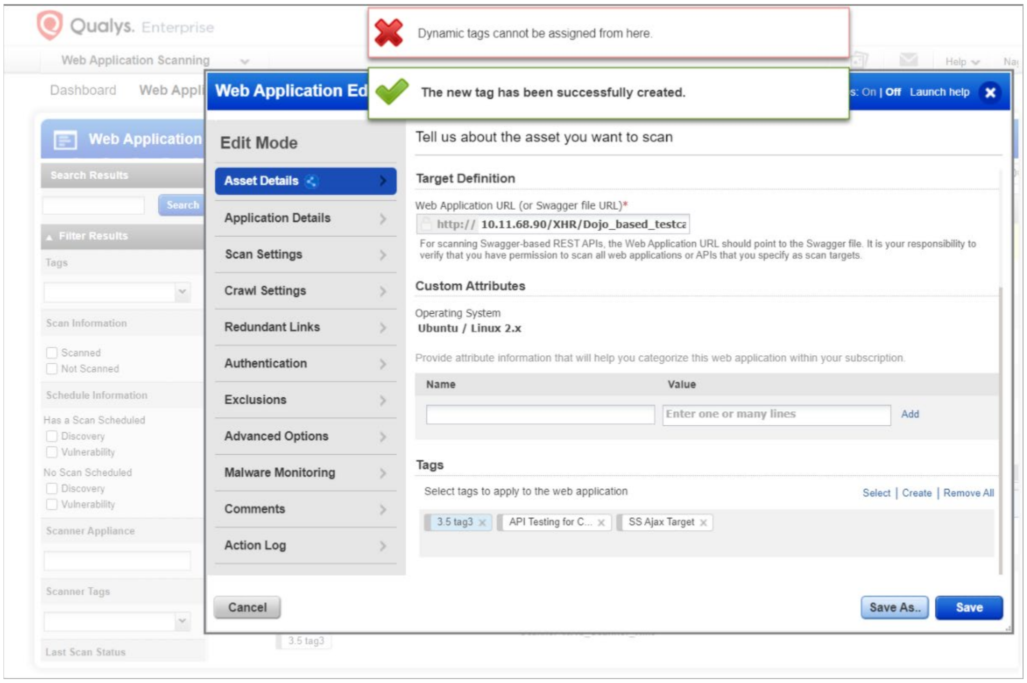
Finding #	3130366(82448934)	Severity	Confirmed Vulnerability - Level 2
Unique #	029a6acd-7ec2-4094-bee8-1ea3c340cd92		
Group	Path Disclosure	Detection Date	19 Jan 2021 10:36 GMT
CWE	CWE-22		
OWASP	A5 Broken Access Control		
WASC	WASC-15 APPLICATION MISCONFIGURATION WASC-16 DIRECTORY INDEXING WASC-17 IMPROPER FILESYSTEM PERMISSIONS		

CVSS V3 Base 5.3 CVSS V3 Temporal5 CVSS V3 Attack Vector Network

Assignment of System Tags and Dynamic Tags Not Supported from WAS UI

You cannot assign System Tags and Dynamic Tags from WAS UI. For example, you cannot assign these tags to web applications, option profiles, DNS overrides, reports and so on. You can add the tags: system and dynamic to the user's scope from the Administration module.

You can create a dynamic tag from UI but if you try to assign this tag to any entity such as web applications, option profiles, DNS overrides, reports, then an error message that "Dynamic tags cannot be assigned from here" will be displayed.



Dynamic tags cannot be assigned from here.

The new tag has been successfully created.

Tell us about the asset you want to scan

Target Definition

Web Application URL (or Swagger file URL)*: http:// 10.11.68.90/XHR/Dojo_based_testca

For scanning Swagger-based REST APIs, the Web Application URL should point to the Swagger file. It is your responsibility to verify that you have permission to scan all web applications or APIs that you specify as scan targets.

Custom Attributes

Operating System: Ubuntu / Linux 2.x

Provide attribute information that will help you categorize this web application within your subscription.

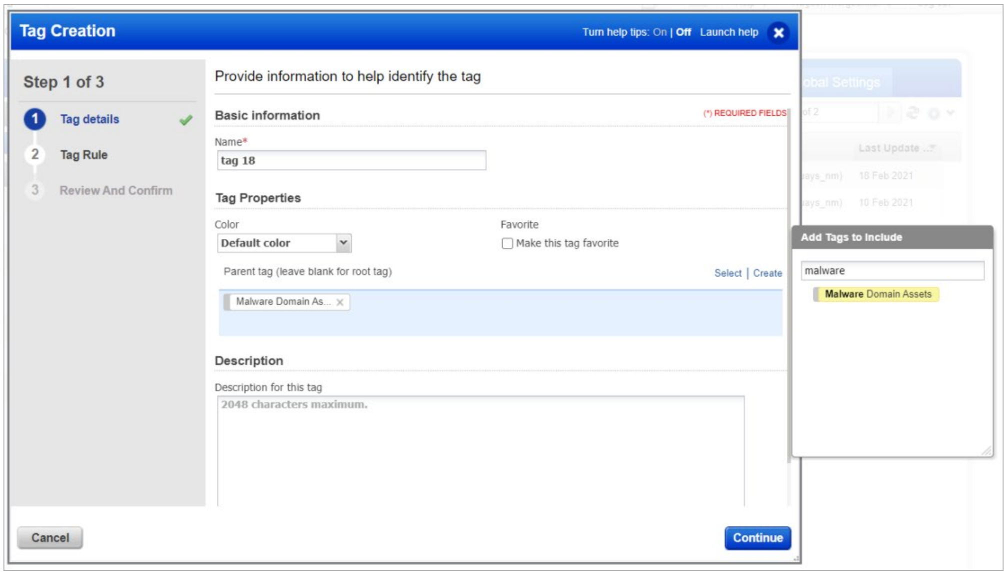
Name	Value
	Enter one or many lines

Tags

Select tags to apply to the web application — Select | Create | Remove All

3.5 tag3 × | API Testing for C... × | SS Ajax Target ×

Though you cannot assign the Dynamic tag, but you can select dynamic tags one for a tag as a parent tag while creating child tag.



Provide information to help identify the tag

Basic information (*) REQUIRED FIELDS

Name*: tag 18

Tag Properties

Color: Default color

Favorite: □ Make this tag favorite

Parent tag (leave blank for root tag) — Select | Create

Malware Domain As... ×

Description

Description for this tag: 2048 characters maximum.

malware

Malware Domain Assets

Global Dashboard Permissions

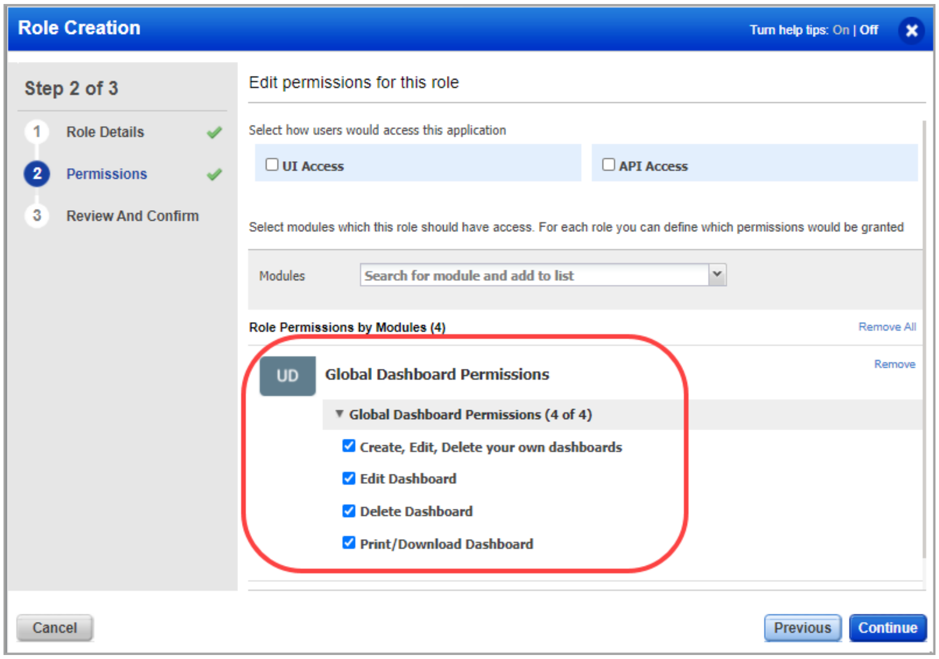
We have now introduced dashboard permissions at a global level. With these global dashboard permissions, you can now assign permissions to users of all modules that have Unified Dashboard (UD) integrated.

The Unified Dashboard framework is a core platform service developed to enhance the data representation and visualization throughout the vision of a ONE Platform ONE Dashboard service. Providing at its core the capability to create widgets from any Qualys supported product in a single dashboard and allowing that same dashboard to be accessed from any module that has migrated to the Unified Dashboard framework.

Currently, UD is integrated with Vulnerability Management Detection and Response (VMDR), Global IT Asset Inventory, File Integrity Management, Patch Management, CertificateView, Endpoint Detection and Response (EDR),.

The Global Dashboard permissions having a higher precedence over module-specific dashboard permissions (only for modules where UD is integrated) and hence it overrides the module-specific dashboard permissions. For example, if Patch Management has only edit dashboard permissions assigned to a role. And if you assign all the permissions in Global dashboard perimssions, users associated with this role will be assigned permissions as per those defined in Global Dashboard.

Go to **Admin** utility > **Users** > **Role Management**. You can edit an existing role or create a new role. In the Modules drop-down, select **Global Dashboard Permissions** and click **Change** to assign the permissions.



Role Creation

Step 2 of 3

1 Role Details ✓

2 Permissions ✓

3 Review And Confirm

Edit permissions for this role

Select how users would access this application

□ UI Access

□ API Access

Select modules which this role should have access. For each role you can define which permissions would be granted

Modules: Search for module and add to list

Role Permissions by Modules (4)

UD Global Dashboard Permissions

▾ Global Dashboard Permissions (4 of 4)

☑ Create, Edit, Delete your own dashboards

☑ Edit Dashboard

☑ Delete Dashboard

☑ Print/Download Dashboard

You can assign the following permissions:

- Create, edit, and delete own dashboards

- Edit dashboards created by other users

- Delete dashboards created by other users

- Print or download dashboards as reports

When a user has multiple roles assigned, the role with highest set of Global Dashboard permissions gets implemented.

For example, if a user John is assigned 3 roles: Admin, Manager, and Reader for separate modules. The Global Dashboard permission for Admin role includes Create, Edit, and Delete your own dashboards, the Manager role has all the permissions assigned, and the Reader role has none of the permissions assigned. In this case, user John is assigned all the permissions of Global Dashboard as per the Manager role. As a result, if previously, user John had read-only permissions for a dashboard in a specific module, user John will now be able to create, edit and delete dashboard across all the modules where UD is integrated.

Dafault Dashboard Permissions:

Depending on the dashboard permissions assigned to the existing role, the default global dashboard permissions are assigned for each role.
- A Manager: All new or existing users with full permissions and scopes are assigned all the permissions.
- A Unit Manager: For existing users with Unit Manager role, the Dashboard permissions from VM/VMDR module are replicated.

Issues Addressed

We have fixed the following issues in this current release-

AV AssetView

- We have fixed an issue where the Search HostAsset API call returned unfiltered results when requesting the output in json (no issue with xml). The API calls now return the results taking into account the fields added to the URL.
- We have fixed an issue where if an asset tag was updated through Update Tag API, it did not reflect the user who updated the asset tag on the UI. Now, the update done through API correctly reflects the user name on the UI.

VMDR Vulnerability Management Detection and Response

- We have fixed an issue where the total vulnerability count vs the vulnerability count by the "Group by Detection Age" filter displayed different values. The vulnerabilities count now matches correctly.

CA Cloud Agent

- Fixed an issue where agent search by 'configurationProfile' was not showing appropriate agent records.

WAS Web Application Scanning

- We fixed an issue where due to a null pointer exception, the user was getting multiple email notifications for a scheduled WAS scan. After the fix, the user receives an email notification only once for the scheduled scan.
- We added a new "<fromAddressOption>" tag to the "Create/Update Schedule API" to let you specify the sender address in the email notification. The From address tag accepts either <fromAddressOption>QUALYS_SUPPORT</fromAddressOption> to specify support@qualys.com or <fromAddressOption>OWNER</fromAddressOption> to specify account owner's email address. For more details refer the WAS API Guide.
- We fixed an issue where the Scan Sitemap was not showing crawl count for some web applications. After the fix, crawl count is displayed in the Scan Sitemap for all the web applications.
- We fixed an issue where the user reported a mismatch between the number of records for the scan data list shown on UI and in the scan data list report that is downloaded using the "Save as Report and download" option. After the fix, the count of records for the scan data list shown on UI and in all formats of the reports is the same.
- We have fixed an issue where the user was getting an error when generating Scan report API. After the fix, you will be able to generate the scan report successfully.