Qualys.

Qualys Cloud Platform v2.x

Release Notes

Version 2.40
July 30, 2019

Here’s what’s new in Qualys Cloud Suite 2.40!

AV AssetView

View current state IOC data

CA Cloud Agent

BSD Support
UDC manifest version in Asset Details

WAS Web Application Scanning

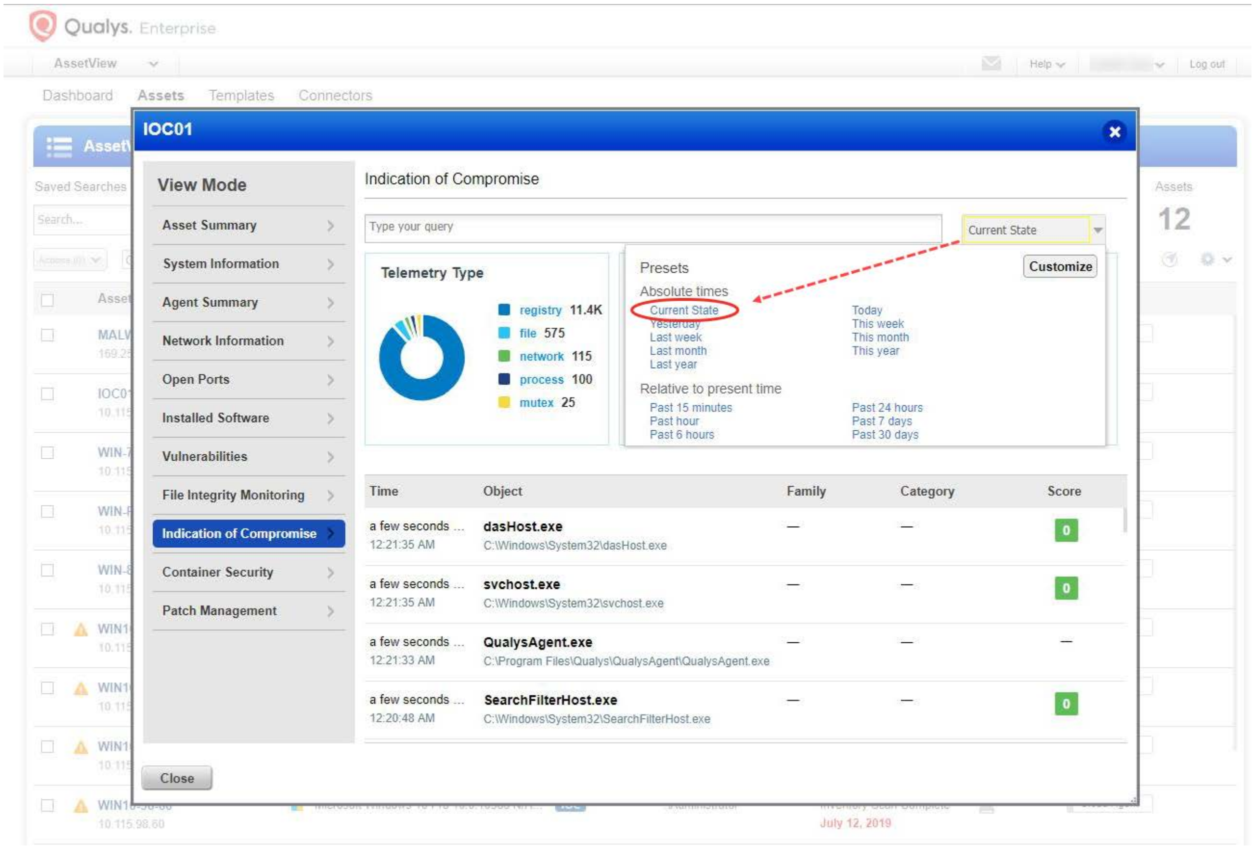
Configure Option Profile with All Detections
Sorting now supported for Multi-Scan
Unique ID for Findings

Qualys Cloud Platform 2.40 brings you many more Improvements and updates! Learn more

View current state IOC data

The Incident of Compromise (IOC) tab of Asset Details now allows to view incident data for the current state.

Select the Current State option from the time picker.



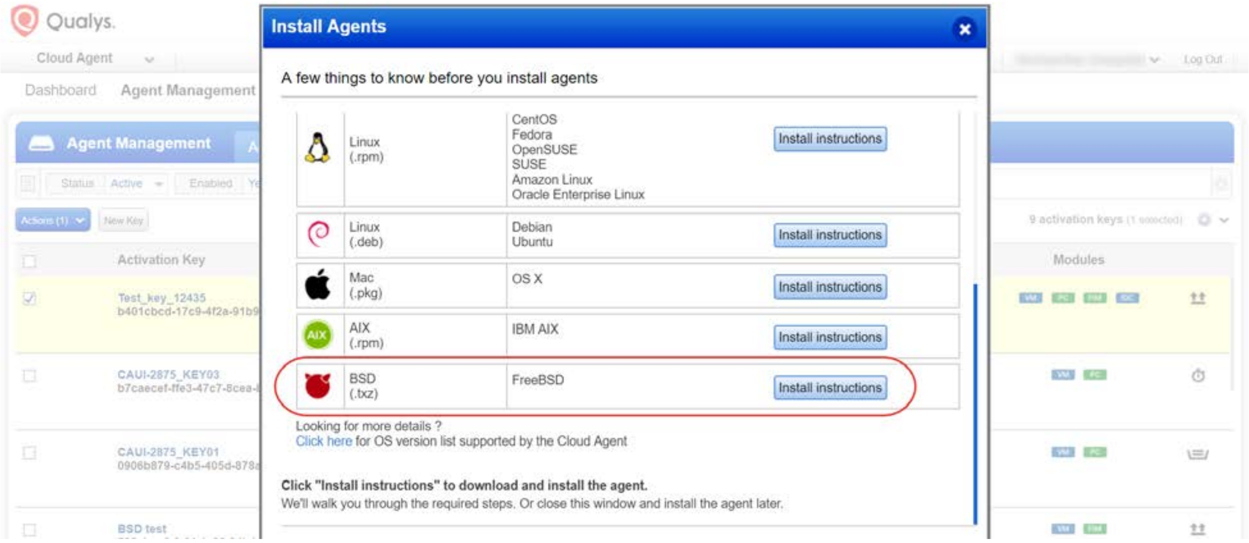
■ registry	11.4K
■ file	575
■ network	115
■ process	100
■ mutex	25

Time	Object	Family	Category	Score
a few seconds ... 12:21:35 AM	dasHost.exe C:\Windows\System32\dasHost.exe	—	—	0
a few seconds ... 12:21:35 AM	svchost.exe C:\Windows\System32\svchost.exe	—	—	0
a few seconds ... 12:21:33 AM	QualysAgent.exe C:\Program Files\Qualys\QualysAgent\QualysAgent.exe	—	—	—
a few seconds ... 12:20:48 AM	SearchFilterHost.exe C:\Windows\System32\SearchFilterHost.exe	—	—	0

CA Cloud Agent

BSD Support

Cloud Agent v2.4.1 now supports BSD versions 10.4 and 11.2. You can download the Cloud Agent installer for BSD from the Qualys Cloud Platform. For more information on BSD support refer to the Qualys Cloud Agent for Linux Installation Guide.



Install Agents

A few things to know before you install agents

	Linux (.rpm)	CentOS Fedora OpenSUSE SUSE Amazon Linux Oracle Enterprise Linux	Install instructions
	Linux (.deb)	Debian Ubuntu	Install instructions
	Mac (.pkg)	OS X	Install instructions
AIX	AIX (.rpm)	IBM AIX	Install instructions
	BSD (.txz)	FreeBSD	Install instructions

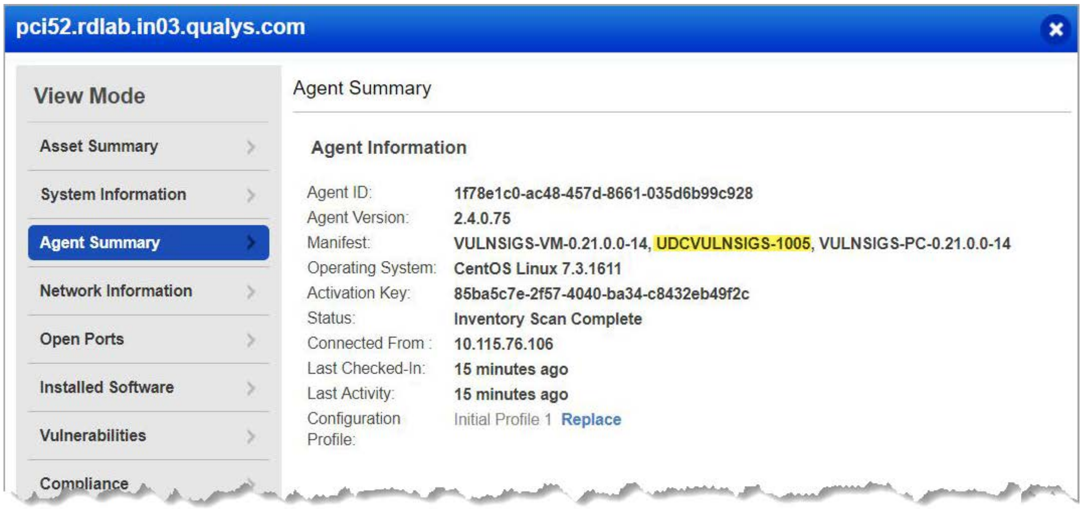
Looking for more details ?
Click here for OS version list supported by the Cloud Agent

Click "Install instructions" to download and install the agent.
We'll walk you through the required steps. Or close this window and install the agent later.

UDC manifest version in Asset Details

Asset Details > Agent Summary will now show the UDC manifest version if you are using User-Defined Controls to scan the asset for compliance.

This information is seen only when the PC module is enabled for your subscription and the Cloud Agent installed on the Asset is activated for PC.



Agent Summary

Agent Information

Agent ID:	1f78e1c0-ac48-457d-8661-035d6b99c928
Agent Version:	2.4.0.75
Manifest:	VULNSIGS-VM-0.21.0.0-14, UDCVULNSIGS-1005, VULNSIGS-PC-0.21.0.0-14
Operating System:	CentOS Linux 7.3.1611
Activation Key:	85ba5c7e-2f57-4040-ba34-c8432eb49f2c
Status:	Inventory Scan Complete
Connected From :	10.115.76.106
Last Checked-In:	15 minutes ago
Last Activity:	15 minutes ago
Configuration Profile:	Initial Profile 1 Replace

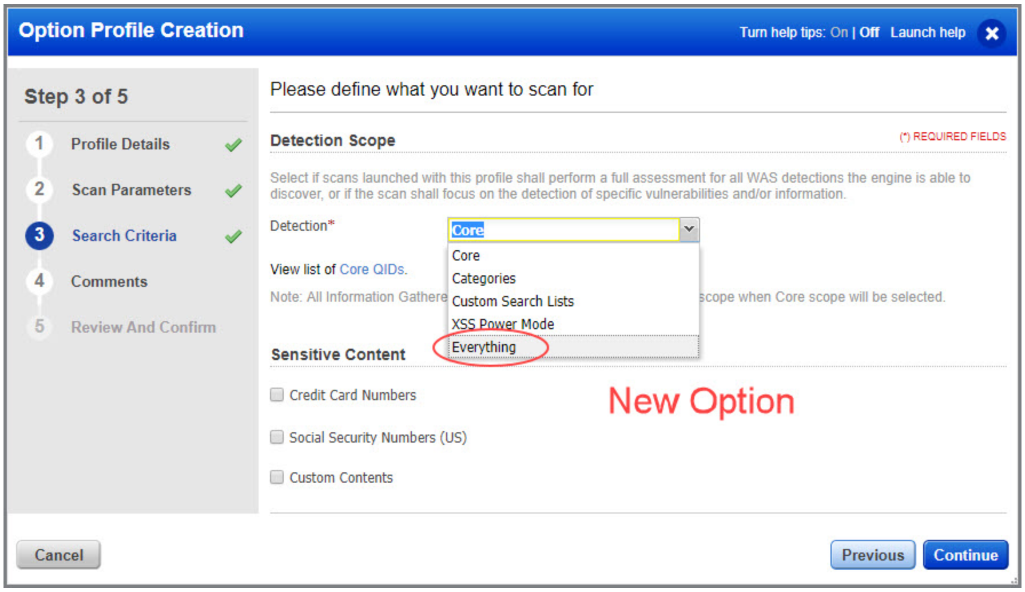
Configure Option Profile with All Detections

You can now configure the detection scope in an option profile for you scan to include all the WAS related detections. The new option named "Everything" (if configured) checks for every WAS related detection during the scan.

How do I configure Everything as detection scope for my scan?

You need to configure the option profile and then choose the configured option profile for the scan.

To configure the option profile, navigate to Configuration > Option Profile. You could either create new option profile or edit an existing one. Choose Everything from the Detection drop-down when you define the search criteria in the option profile configuration.



Option Profile Creation

Step 3 of 5

Please define what you want to scan for

Detection Scope

(*) REQUIRED FIELDS

Select if scans launched with this profile shall perform a full assessment for all WAS detections the engine is able to discover, or if the scan shall focus on the detection of specific vulnerabilities and/or information.

Detection*: Core

View list of Core QIDs.

Note: All Information Gathere scope when Core scope will be selected.

Sensitive Content

□ Credit Card Numbers

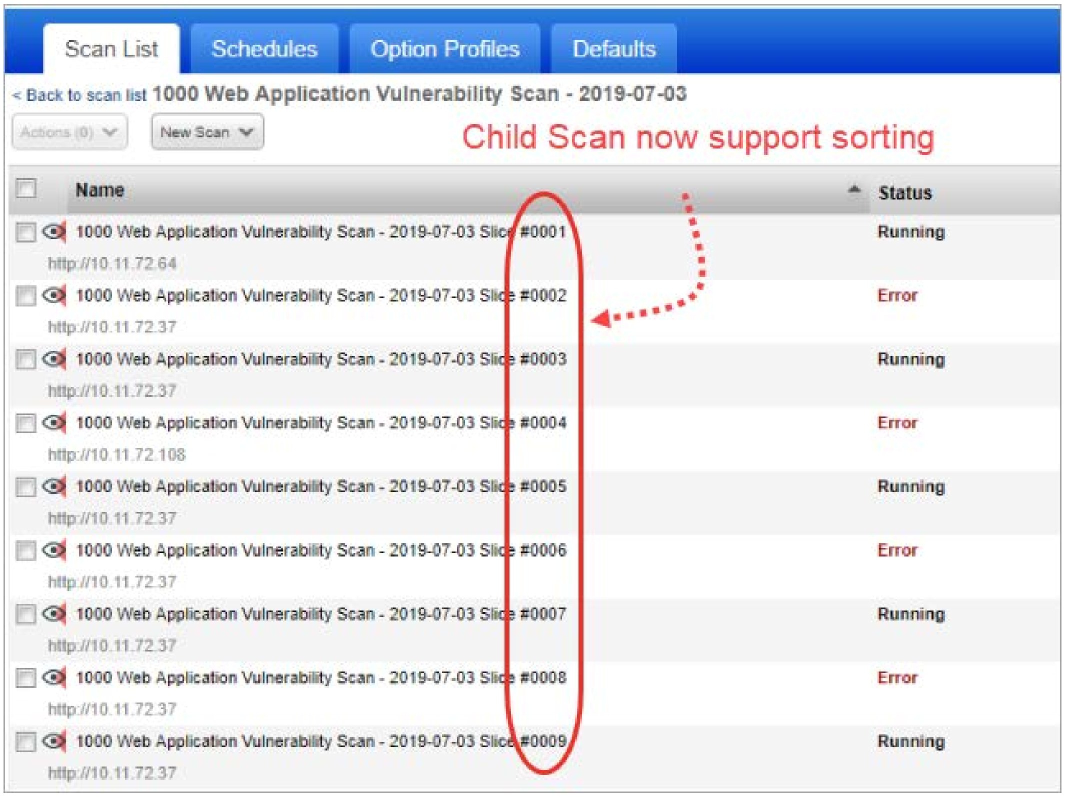
□ Social Security Numbers (US)

□ Custom Contents

Note: Choosing Everything in detection scope implies that the scan will check for all the WAS related vulnerabilities and this could lead to a longer scan time.

Sorting now supported for Multi-Scan

You can now sort the child scans in a multi-scan to display in ascending sequence. Earlier the child scan numbering format was such that they were listed randomly. Now, you can sort the child scans and get them listed in ascending sequence.



< Back to scan list **1000 Web Application Vulnerability Scan - 2019-07-03**

Child Scan now support sorting

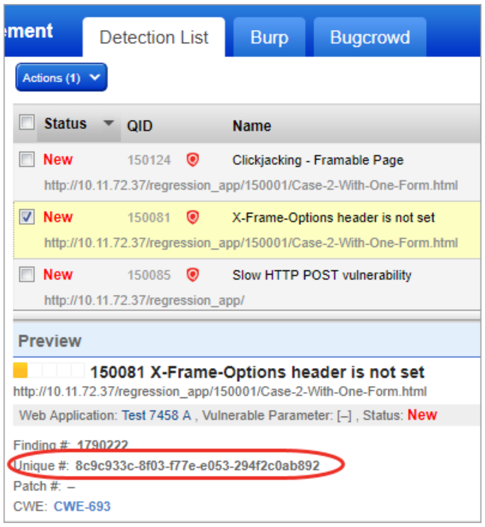
□	Name	Status
□	1000 Web Application Vulnerability Scan - 2019-07-03 Slice #0001 http://10.11.72.64	Running
□	1000 Web Application Vulnerability Scan - 2019-07-03 Slice #0002 http://10.11.72.37	Error
□	1000 Web Application Vulnerability Scan - 2019-07-03 Slice #0003 http://10.11.72.37	Running
□	1000 Web Application Vulnerability Scan - 2019-07-03 Slice #0004 http://10.11.72.108	Error
□	1000 Web Application Vulnerability Scan - 2019-07-03 Slice #0005 http://10.11.72.37	Running
□	1000 Web Application Vulnerability Scan - 2019-07-03 Slice #0006 http://10.11.72.37	Error
□	1000 Web Application Vulnerability Scan - 2019-07-03 Slice #0007 http://10.11.72.37	Running
□	1000 Web Application Vulnerability Scan - 2019-07-03 Slice #0008 http://10.11.72.37	Error
□	1000 Web Application Vulnerability Scan - 2019-07-03 Slice #0009 http://10.11.72.37	Running

Unique ID for Findings

We have now introduced 36-bit unique ID (uniqueId) for each finding. The ID would be unique for every finding. Earlier, the combination of three fields namely: finding ID, finding type and finding category would make a finding unique. Now, with the implementation of uniqueId, you can easily distinguish every finding.

Preview section of a Detection

Navigate to Detections tab an select a detection. You will notice the Unique# in the preview section. Every detection is now assigned a 36 bit unique ID.



	Status	QID	Name
□	New	150124	Clickjacking - Framable Page
	http://10.11.72.37/regression_app/150001/Case-2-With-One-Form.html		
☑	New	150081	X-Frame-Options header is not set
	http://10.11.72.37/regression_app/150001/Case-2-With-One-Form.html		
□	New	150085	Slow HTTP POST vulnerability
	http://10.11.72.37/regression_app/		

Preview

150081 X-Frame-Options header is not set

http://10.11.72.37/regression_app/150001/Case-2-With-One-Form.html

Web Application: Test 7458 A , Vulnerable Parameter: [–] , Status: New

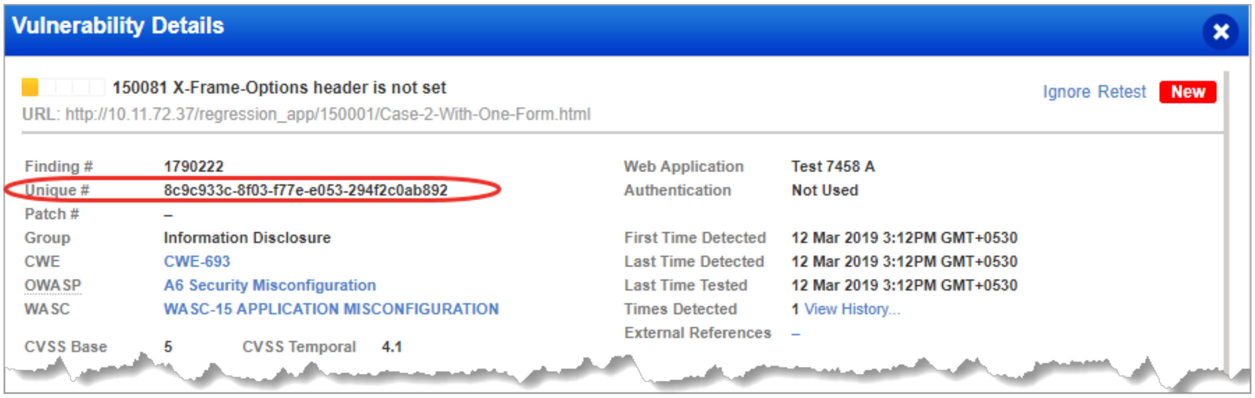
Finding #: 1790222

Unique #: 8c9c933c-8f03-f77e-e053-294f2c0ab892

Patch #: –

CWE: CWE-693

Vulnerability Details



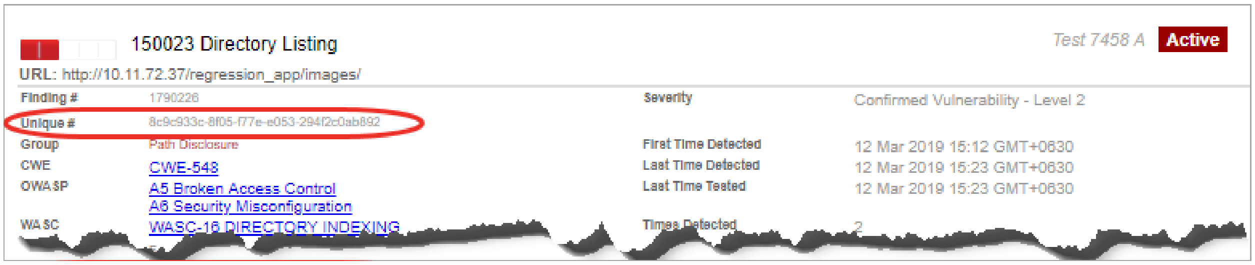
150081 X-Frame-Options header is not set

URL: http://10.11.72.37/regression_app/150001/Case-2-With-One-Form.html

Finding #	1790222	Web Application	Test 7458 A
Unique #	8c9c933c-8f03-f77e-e053-294f2c0ab892	Authentication	Not Used
Patch #	–		
Group	Information Disclosure	First Time Detected	12 Mar 2019 3:12PM GMT+0530
CWE	CWE-693	Last Time Detected	12 Mar 2019 3:12PM GMT+0530
OWASP	A6 Security Misconfiguration	Last Time Tested	12 Mar 2019 3:12PM GMT+0530
WASC	WASC-15 APPLICATION MISCONFIGURATION	Times Detected	1 View History...
		External References	–
CVSS Base	5 CVSS Temporal 4.1		

The reports also now displays the unique ID assigned to a detection.

Sample: Web Application Report in HTML format



150023 Directory Listing

Test 7458 A

URL: http://10.11.72.37/regression_app/images/

Finding #	1790226	Severity	Confirmed Vulnerability - Level 2
Unique #	8c9c933c-8f05-f77e-e053-294f2c0ab892		
Group	Path Disclosure	First Time Detected	12 Mar 2019 15:12 GMT+0630
CWE	CWE-548	Last Time Detected	12 Mar 2019 15:23 GMT+0630
OWASP	A5 Broken Access Control A6 Security Misconfiguration	Last Time Tested	12 Mar 2019 15:23 GMT+0630
WASC	WASC-16 DIRECTORY INDEXING	Times Detected	2

Issues addressed in this release

Qualys Cloud Platform 2.40 brings you many more improvements and updates.

AV AssetView

- Fixed an issue where changes made to the dashboard layout were getting lost upon page refresh.
- Fixed an issue where saving a widget displayed a save error.
- Fixed an issue in Asset Details where the IOC panel did not show any data.
- Fixed an issue where the asset list did not show a proper icon for assets added through SEM (Mobile operating systems).
- Fixed an issue where downloaded reports showed Activity status as "Agent Error".
- We have updated the description with correct states for connectorState parameter in Asset Management and Tagging API User Guide.
- We have updated the topics related to Azure Connector in AssetView online help to reflect the latest changes on the Azure portal.

CA Cloud Agent

- A proper error message is now displayed when a user tries to delete a configuration profile assigned to an agent.
- Activation key limit count will now be 0 if agent provision exceeds beyond the key limit.

WAS Web Application Scanning

- We have now fixed the Web Application Report to display the Detection Source (which was earlier hidden) in the Web Application Report.
- Despite multiple (more than 3) DNS override done on the UI, the UI reflected only 3 DNS override. We have now fixed the issue to correctly reflect the all DNS overrides now on the UI.
- The Scan report when opened with "open in a new window" option displayed an error. Now, it is correctly displayed in a new window without any errors.
- We updated the response with user-friendly example for "Sample - Create a standard authentication record" in WAS API User Guide.
- We have fixed multiple issues for Finding API:
  - The vulnerabilities and IG's can now be identified using a combination of <id>, <type> and findingType> filters.
  - When user uses the following filter in Finding API, only vulnerabilities are correctly displayed in the API response.
  <Criteria field="type" operator="EQUALS">VULNERABILITY</Criteria>

- We now utilize the full space to display the URL for a vulnerability in the Detections list. Earlier, the URL was truncated with ample space available under name column.
- The Last Time Tested & Last Time Detected fields in Vulnerability Details displayed incorrect dates when a retest scan failed. We have now fixed the issue to display the correct dates for Last Time Tested & Last Time Detected even if the retest fails.

Qualys Cloud Platform

- Updated the AM & Tagging API guide to remove the mention of POST method for Get Host Asset Info and Get Asset Info APIs. These APIs only support the GET method.
- The log of tag updated using API didn't reflect in action log of the tag. We have rectified the issue and have now introduced a column named Source in Action Log to reflect the source (UI or API).