Update On Enhanced Oracle Java Discovery

Dec, 2020

Qualys, Inc.
919 E Hillsdale Blvd 4th Floor
Foster City, CA 94404
1 (650) 801 6100

About This Document

This document provides details related to the Enhanced Oracle Java Discovery a new capability implemented by Qualys Research team.

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions. The Qualys Cloud Platform and its integrated apps help businesses simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance and protection for IT systems and web applications.

Founded in 1999, Qualys has established strategic partnerships with leading managed service providers and consulting organizations including Accenture, BT, Cognizant Technology Solutions, Deutsche Telekom, Fujitsu, HCL, HP Enterprise, IBM, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon and Wipro. The company is also founding member of the Cloud Security Alliance (CSA). For more information, please visit www.qualys.com.

What Happened?

On Dec 10th Qualys research team released an update to its signatures to detect Oracle Java instances installed in non-standard locations. As a result of this change, customers saw an increased number of Oracle Java vulnerabilities being reported in their environment negatively impacting their year-end compliance posture reporting.

Why were the changes implemented?

The Qualys research team is continuously looking for better ways to identify and accurately report vulnerabilities. As part of this effort, and also based on customer requests we updated Oracle Java vulnerability detection logic to give our customers better visibility into vulnerable instances of Oracle Java installed in non-standard locations.

What was the impact of the change?

Customers saw an increased number of Oracle Java vulnerabilities that were installed in non-standard locations.

What steps is Qualys taking to help customers?

Qualys research team has created a detailed blog explaining the new detection logic for QIDs for Oracle Java, and has also laid out scenarios where these QIDs will be reported as vulnerable.

We have also added a FAQ section to the blog, which answers frequently asked questions from our customers. We will continue to update the FAQ section based on input from customers.

How have Qualys customers reacted to this change?

Qualys customers are appreciative of the fact that these changes bring in required visibility into Oracle Java vulnerabilities in instances installed in non-standard locations that were not reported earlier. But they requested going forward to have a pre-notification for such changes. Which we are implementing right away.

Which Oracle Java QID's were impacted by this update?

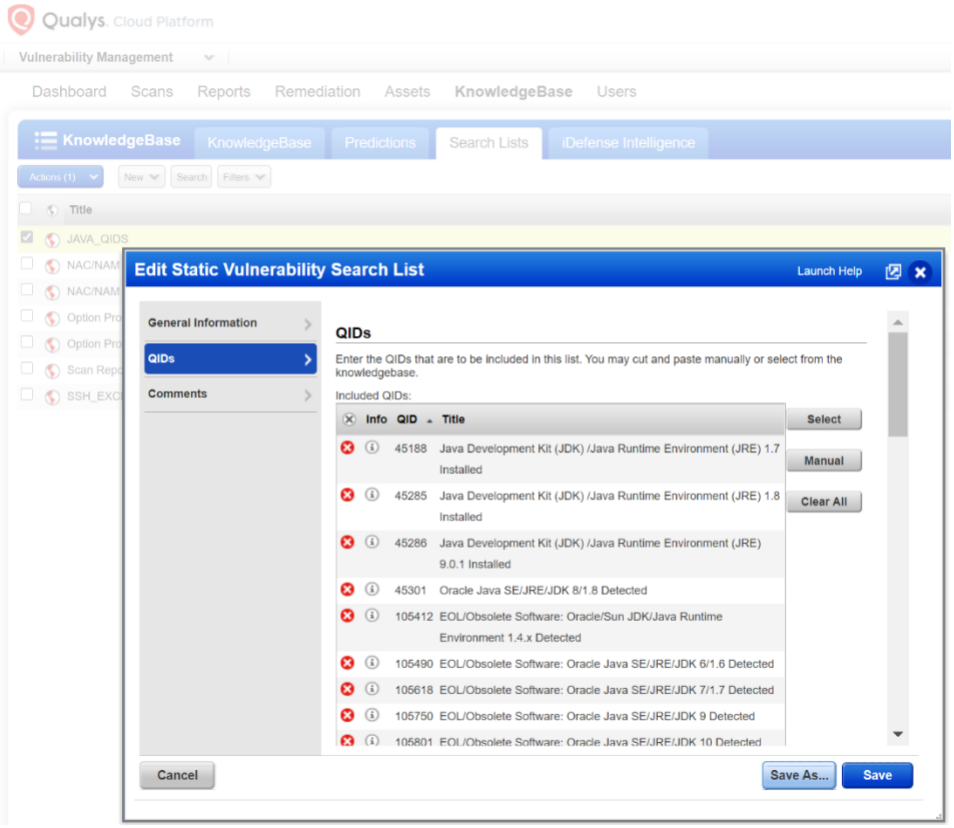
The Following list of QIDs were impacted as part of this change.

119956, 120274, 120443, 120443, 120604, 120799, 120832, 45188, 120879, 120970, 121061, 105490, 121279, 121515, 121712, 122007, 122362, 122741, 123168, 123519, 105618, 123714, 124169, 124567, 124882, 370087, 370161, 370280, 370371, 370469, 370610, 45285, 45286, 370727, 45301, 370887, 105750, 371079, 371265, 371528, 371749, 105801, 372013, 372163, 372333, 372508, 373156, 373540, 105412

What options are available to exclude the Oracle Java QID's from reporting?

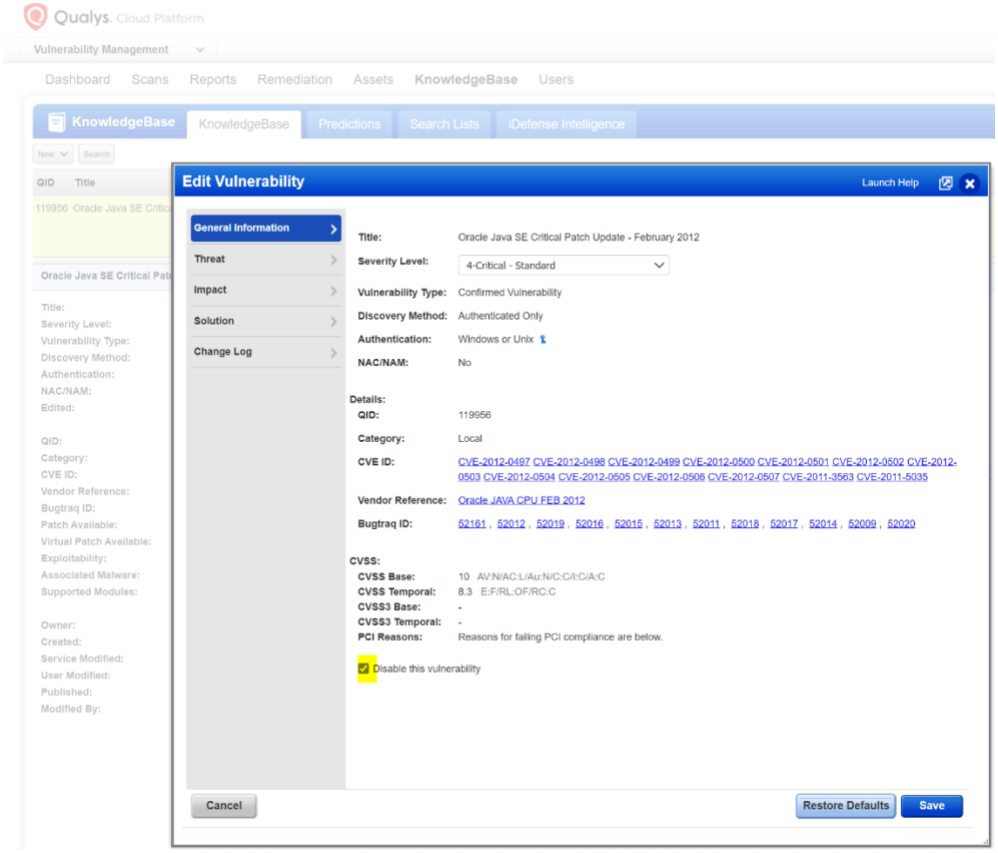
Two options to exclude QID's.

1. Use a Static Search List to filter out Java QID's from reporting.
    a. In the next section, we'll cover multiple options to filter out the list of Java QID's impacted by this update. Below is an example of where to create your search list:



2. Temporarily Disable the list of Java QIDs in the KnowledgeBase.
    a. All Reporting through UI, and API will exclude the QID's unless they are explicitly included.
    b. Enable the QID's once you are ready to process data.

c. Below is an example of temporarily disabling the vulnerability.

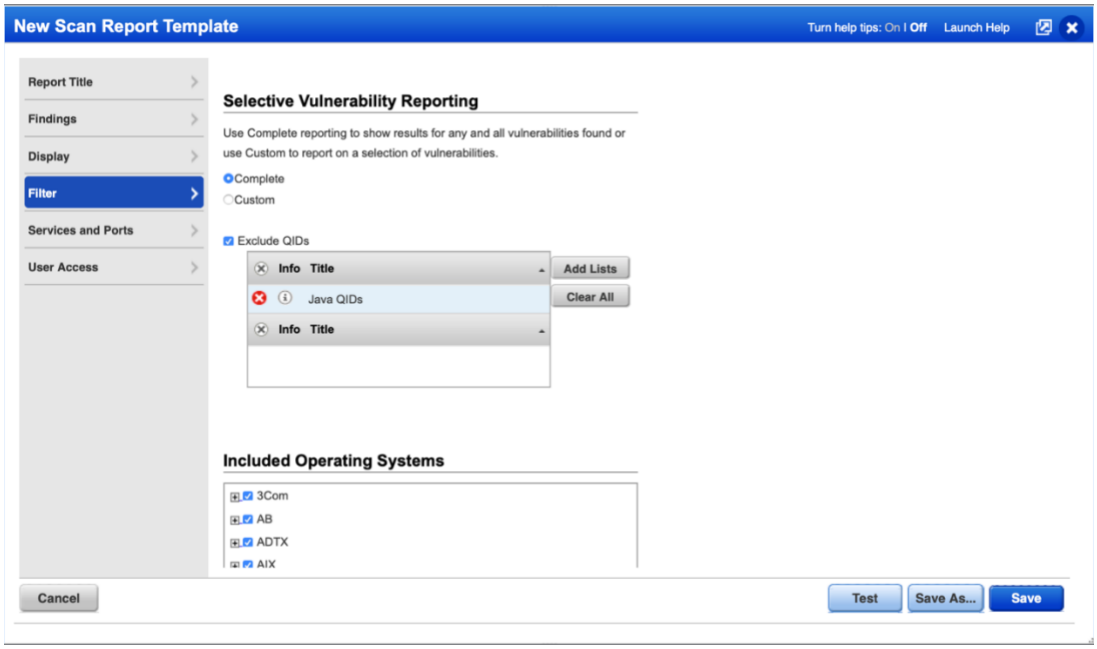


What options in reporting and widgets are available to identify or filter out these detections?

There are multiple options to identify and filter out Oracle Java detections.

1. **Filter detections using Exclude QIDs from the reporting UI**

   Customers can choose to temporarily exclude findings from these QIDs using Report Templates and search lists to reduce impact on end of year reporting metrics.



2. **Filter detections using the API**

   Use the API to call the report created above to exclude the QIDs.

   https://www.qualys.com/docs/qualys-api-vmpc-user-guide.pdf (refer to pg. 475 & 513)

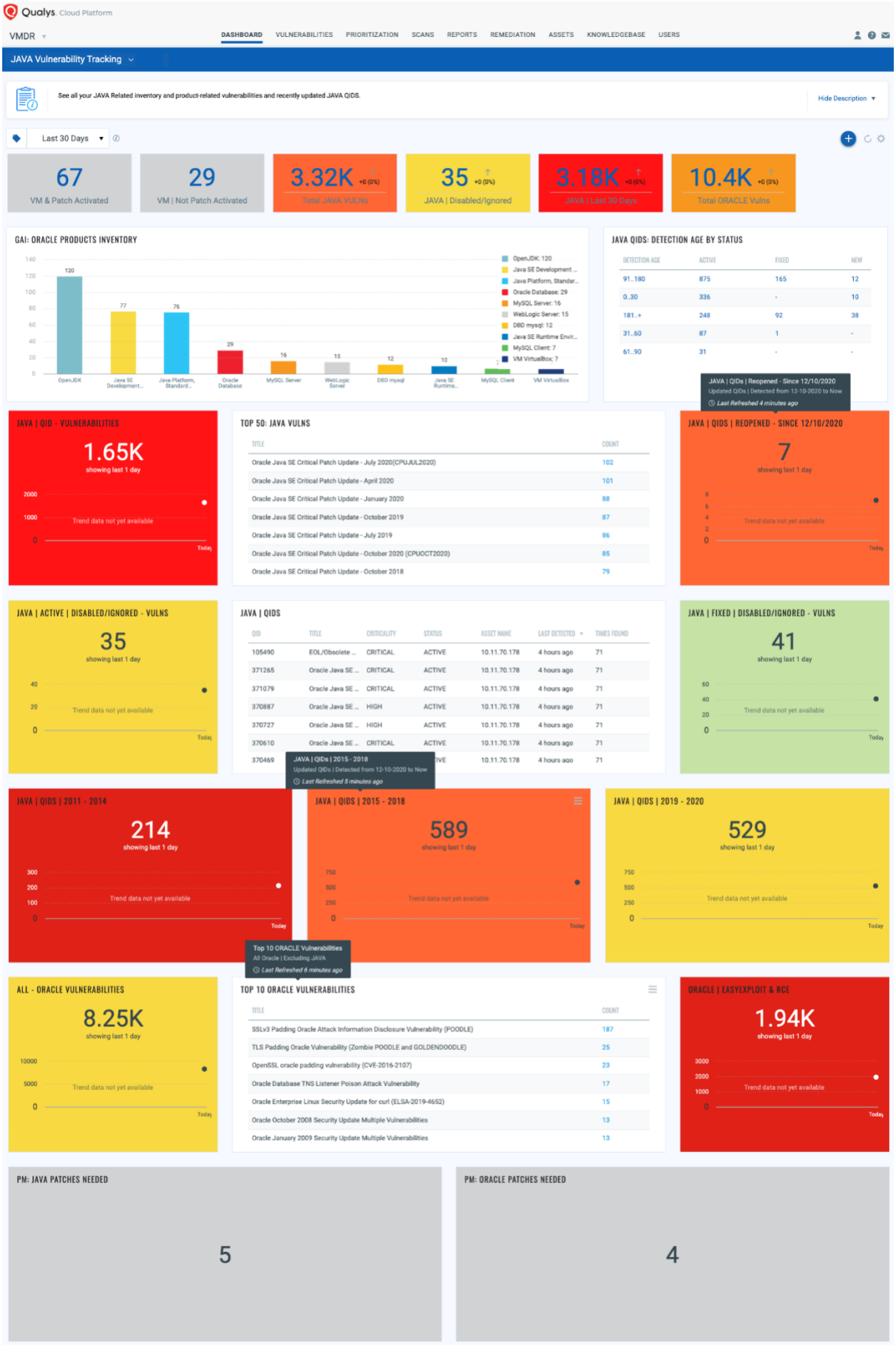
3. **Use Remediation Policies and Report Templates to exclude QIDs**

   Review the following videos to exclude the QIDs using remediation policies.

   https://vimeo.com/341663056 (Remediation Policies)
   https://vimeo.com/341661423 (Report Templates)

How can I track these changes through a Dashboard in VMDR?

With Qualys Unified Dashboard, you can track Java vulnerabilities, impacted hosts, their status and overall management in real time. Enable trending so you can keep track of these vulnerability trends across your environments.
Dashboard: Java QIDs and All Java Vulnerabilities!


Qualys. Cloud Platform
VMDR
DASHBOARD
VULNERABILITIES
PRIORITIZATION
SCANS
REPORTS
REMEDIATION
ASSETS
KNOWLEDGEBASE
USERS
JAVA Vulnerability Tracking
See all your JAVA Related inventory and product-related vulnerabilities and recently updated JAVA QIDS.
Hide Description
Last 30 Days
67
VM & Patch Activated
29
VM | Not Patch Activated
3.32K
Total JAVA VULNs
35
JAVA | Disabled/Ignored
3.18K
JAVA | Last 30 Days
10.4K
Total ORACLE Vulns
GAI: ORACLE PRODUCTS INVENTORY
OpenJDK: 120
Java SE Development ...
Java Platform, Standar...
Oracle Database: 29
MySQL Server: 16
WebLogic Server: 15
DBD mysql: 12
Java SE Runtime Envir...
MySQL Client: 7
VM VirtualBox: 7
JAVA QIDS: DETECTION AGE BY STATUS
DETECTION AGE
ACTIVE
FIXED
NEW
91..180
875
165
12
0..30
336
-
10
181..+
248
92
38
31..60
87
1
-
61..90
31
-
-
JAVA | QIDs | Reopened - Since 12/10/2020
Updated QIDs | Detected from 12-10-2020 to Now
Last Refreshed 4 minutes ago
JAVA | QID - VULNERABILITIES
1.65K
showing last 1 day
Trend data not yet available
Today
TOP 50: JAVA VULNS
TITLE
COUNT
Oracle Java SE Critical Patch Update - July 2020(CPUJUL2020)
102
Oracle Java SE Critical Patch Update - April 2020
101
Oracle Java SE Critical Patch Update - January 2020
88
Oracle Java SE Critical Patch Update - October 2019
87
Oracle Java SE Critical Patch Update - July 2019
86
Oracle Java SE Critical Patch Update - October 2020 (CPUOCT2020)
85
Oracle Java SE Critical Patch Update - October 2018
79
JAVA | QIDS | REOPENED - SINCE 12/10/2020
7
showing last 1 day
Trend data not yet available
Today
JAVA | ACTIVE | DISABLED/IGNORED - VULNS
35
showing last 1 day
Trend data not yet available
Today
JAVA | QIDS
QID
TITLE
CRITICALITY
STATUS
ASSET NAME
LAST DETECTED
TIMES FOUND
105490
EOL/Obsolete ...
CRITICAL
ACTIVE
10.11.70.178
4 hours ago
71
371265
Oracle Java SE ...
CRITICAL
ACTIVE
10.11.70.178
4 hours ago
71
371079
Oracle Java SE ...
CRITICAL
ACTIVE
10.11.70.178
4 hours ago
71
370887
Oracle Java SE ...
HIGH
ACTIVE
10.11.70.178
4 hours ago
71
370727
Oracle Java SE ...
HIGH
ACTIVE
10.11.70.178
4 hours ago
71
370610
Oracle Java SE ...
CRITICAL
ACTIVE
10.11.70.178
4 hours ago
71
370469
10.11.70.178
4 hours ago
71
JAVA | QIDs | 2015 - 2018
Updated QIDs | Detected from 12-10-2020 to Now
Last Refreshed 5 minutes ago
JAVA | FIXED | DISABLED/IGNORED - VULNS
41
showing last 1 day
Trend data not yet available
Today
JAVA | QIDS | 2011 - 2014
214
showing last 1 day
Trend data not yet available
Today
JAVA | QIDS | 2015 - 2018
589
showing last 1 day
Trend data not yet available
Today
JAVA | QIDS | 2019 - 2020
529
showing last 1 day
Trend data not yet available
Today
Top 10 ORACLE Vulnerabilities
All Oracle | Excluding JAVA
Last Refreshed 6 minutes ago
ALL - ORACLE VULNERABILITIES
8.25K
showing last 1 day
Trend data not yet available
Today
TOP 10 ORACLE VULNERABILITIES
TITLE
COUNT
SSLv3 Padding Oracle Attack Information Disclosure Vulnerability (POODLE)
187
TLS Padding Oracle Vulnerability (Zombie POODLE and GOLDENDOODLE)
25
OpenSSL oracle padding vulnerability (CVE-2016-2107)
23
Oracle Database TNS Listener Poison Attack Vulnerability
17
Oracle Enterprise Linux Security Update for curl (ELSA-2019-4652)
15
Oracle October 2008 Security Update Multiple Vulnerabilities
13
Oracle January 2009 Security Update Multiple Vulnerabilities
13
ORACLE | EASYEXPLOIT & RCE
1.94K
showing last 1 day
Trend data not yet available
Today
PM: JAVA PATCHES NEEDED
5
PM: ORACLE PATCHES NEEDED
4

How would this change impact status of QIDs detected with old detection logic?

The QID status will continue to follow standard QID status workflow. Please review following link for more details.

https://qualysguard.qg2.apps.qualys.com/qwebhelp/fo_portal/scans/vulnerability_status.htm

How will Qualys notify customers of similar changes in future?

Qualys research team will implement a 15-day notification process for any bulk modification of QIDs or significant changes to underlying QID detection logic for major applications.

https://notifications.qualys.com

Will Qualys add similar detection support for other technologies?

Yes. Qualys research team plans to add similar detection capabilities for other technologies. The team will provide a 15-day notification before such changes are made live. In addition to that we will allow customers to opt-in into enhanced detection capabilities in future.