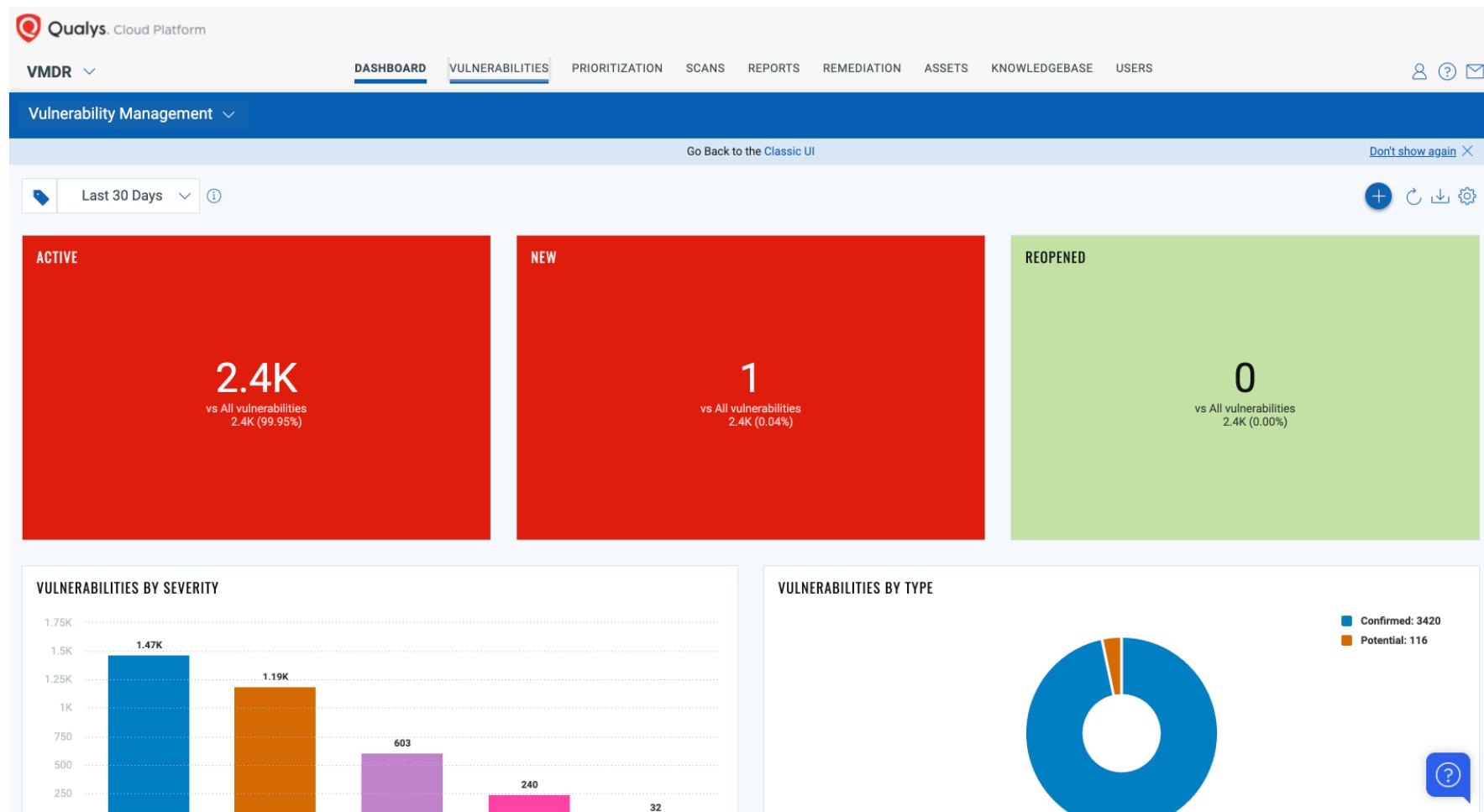




007 - Vulnerability Findings

- Vulnerability findings (for all assets) can be viewed from the VULNERABILITIES section of Qualys VM and VMDR. Near the top of the page, click **VULNERABILITIES**.





007 - Vulnerability Findings



All detected vulnerabilities are listed here.

Qualys Cloud Platform

VMDR ▾ DASHBOARD VULNERABILITIES PRIORITIZATION SCANS REPORTS REMEDIATION ASSETS KNOWLEDGEBASE USERS

Vulnerabilities

2.41K Total Detections

SEVERITY

Severity	Count
4	954
3	945
5	314
2	181
1	16

CATEGORY

Category	Count
OEL	691
Windows	630
Local	362
CentOS	278
Internet Explorer	203
11 more ▾	

OPERATING SYSTEM

Operating System	Count
Oracle Enterprise...	438
Windows Server ...	437
CentOS 6.5	397
Windows 10 Pro ...	372
x86_64 Linux/2.6...	266
11 more ▾	

TYPE DETECTED

Type Detected	Count
OpenSSH	2.39K

Vulnerability ▾ Search... [+] [?] [≡]

Actions (0) ▾ Asset Vulnerability Group by ... ▾ Filters ▾ 1 - 200 of 2410 [refresh] [down] [left] [right] [gear]

QID	Title	Severity	Last Detected	First Detected	Asset
105936	OpenSSH Command Injection Vulnerability (Generic) Active	██████	Oct 11, 2021	Mar 20, 2021	ip-172-31-7-120... 324815310
352851	Amazon Linux Security Advisory for ca-certificates: ALAS2-2021-1710 Active	██████	Oct 11, 2021	Oct 06, 2021	ip-172-31-7-120... 324815310
352836	Amazon Linux Security Advisory for openldap: ALAS2-2021-1707 Active	██████	Oct 11, 2021	Sep 21, 2021	ip-172-31-7-120... 324815310
352839	Amazon Linux Security Advisory for kernel: ALAS2-2021-1704 Active	██████	Oct 11, 2021	Sep 21, 2021	ip-172-31-7-120... 324815310
352840	Amazon Linux Security Advisory for glibc: ALAS2-2021-1703 Active	██████	Oct 11, 2021	Sep 21, 2021	ip-172-31-7-120... 324815310
352843	Amazon Linux Security Advisory for curl: ALAS2-2021-1700 Active	██████	Oct 11, 2021	Sep 21, 2021	ip-172-31-7-120... 324815310
352799	Amazon Linux Security Advisory for kernel: ALAS2-2021-1699 Active	██████	Oct 11, 2021	Sep 13, 2021	ip-172-31-7-120... 324815310
352506	Amazon Linux Security Advisory for curl: ALAS2-2021-1693 Active	██████	Oct 11, 2021	Aug 12, 2021	ip-172-31-7-120... 324815310
352503	Amazon Linux Security Advisory for kernel: ALAS2-2021-1696 Active	██████	Oct 11, 2021	Aug 12, 2021	ip-172-31-7-120... 324815310
352500	Amazon Linux Security Advisory for kernel: ALAS2-2021-1691 Active	██████	Oct 11, 2021	Jul 29, 2021	ip-172-31-7-120... 324815310
352485	Amazon Linux Security Advisory for curl: ALAS2-2021-1680	██████	Oct 11, 2021	Jul 05, 2021	ip-172-31-7-120... 324815310



007 - Vulnerability Findings



You can toggle the view between Vulnerabilities or their associated Assets. For now, we'll stick with vulnerabilities.

The screenshot shows the Qualys Cloud Platform interface for vulnerability management. The top navigation bar includes links for VMDR, DASHBOARD, VULNERABILITIES (which is currently selected), PRIORITIZATION, SCANS, REPORTS, REMEDIATION, ASSETS, KNOWLEDGEBASE, and USERS. A search bar and filter options are available at the top right. On the left, there's a sidebar with summary statistics: 2.41K Total Detections, Severity counts (4: 954, 3: 945, 5: 314, 2: 181, 1: 16), Category counts (OEL: 691, Windows: 630, Local: 362, CentOS: 278, Internet Explorer: 203, 11 more), Operating System counts (Oracle Enterprise: 438, Windows Server: 437, CentOS 6.5: 397, Windows 10 Pro: 372, x86_64 Linux/2.6: 266, 11 more), and Type Detected counts (General: 0, OS: 0, App: 0). The main content area displays a table of vulnerabilities with columns for ID, Title, Severity, Last Detected, First Detected, and Asset. The 'Asset' button in the toolbar is highlighted with a red box. The table lists several entries, such as OpenSSH Command Injection Vulnerability (Generic) and various Amazon Linux Security Advisories.

ID	Title	Severity	Last Detected	First Detected	Asset
105936	OpenSSH Command Injection Vulnerability (Generic) Active	High	Oct 11, 2021	Mar 20, 2021	ip-172-31-7-120... 324815310
352851	Amazon Linux Security Advisory for ca-certificates: ALAS2-2021-1710 Active	High	Oct 11, 2021	Oct 06, 2021	ip-172-31-7-120... 324815310
352836	Amazon Linux Security Advisory for openldap: ALAS2-2021-1707 Active	High	Oct 11, 2021	Sep 21, 2021	ip-172-31-7-120... 324815310
352839	Amazon Linux Security Advisory for kernel: ALAS2-2021-1704 Active	High	Oct 11, 2021	Sep 21, 2021	ip-172-31-7-120... 324815310
352840	Amazon Linux Security Advisory for glibc: ALAS2-2021-1703 Active	High	Oct 11, 2021	Sep 21, 2021	ip-172-31-7-120... 324815310
352843	Amazon Linux Security Advisory for curl: ALAS2-2021-1700 Active	High	Oct 11, 2021	Sep 21, 2021	ip-172-31-7-120... 324815310
352799	Amazon Linux Security Advisory for kernel: ALAS2-2021-1699 Active	High	Oct 11, 2021	Sep 13, 2021	ip-172-31-7-120... 324815310
352506	Amazon Linux Security Advisory for curl: ALAS2-2021-1693 Active	High	Oct 11, 2021	Aug 12, 2021	ip-172-31-7-120... 324815310
352503	Amazon Linux Security Advisory for kernel: ALAS2-2021-1696 Active	High	Oct 11, 2021	Aug 12, 2021	ip-172-31-7-120... 324815310
352500	Amazon Linux Security Advisory for kernel: ALAS2-2021-1691 Active	High	Oct 11, 2021	Jul 29, 2021	ip-172-31-7-120... 324815310



007 - Vulnerability Findings

-  The total number of detections are listed at the top of the faceted search pane.

Qualys Cloud Platform

VMDR DASHBOARD VULNERABILITIES PRIORITIZATION SCANS REPORTS REMEDIATION ASSETS KNOWLEDGEBASE USERS

Vulnerabilities

2.41K Total Detections

SEVERITY

4	954
3	945
5	314
2	181
1	16

CATEGORY

OEL	691
Windows	630
Local	362
CentOS	278
Internet Explorer	203
11 more	▼

OPERATING SYSTEM

Oracle Enterprise...	438
Windows Server ...	437
CentOS 6.5	397
Windows 10 Pro ...	372
x86_64 Linux/2.6...	266
11 more	▼

TYPE DETECTED

OpenSSH	2,381
Apache	1,023
curl	832
nginx	711
curl	640
OpenSSL	559
OpenBSD	550
OpenSSH	540
OpenSSL	530
curl	520
OpenSSL	510
curl	500
OpenSSL	490
curl	480
OpenSSL	470
curl	460
OpenSSL	450
curl	440
OpenSSL	430
curl	420
OpenSSL	410
curl	400
OpenSSL	390
curl	380
OpenSSL	370
curl	360
OpenSSL	350
curl	340
OpenSSL	330
curl	320
OpenSSL	310
curl	300
OpenSSL	290
curl	280
OpenSSL	270
curl	260
OpenSSL	250
curl	240
OpenSSL	230
curl	220
OpenSSL	210
curl	200
OpenSSL	190
curl	180
OpenSSL	170
curl	160
OpenSSL	150
curl	140
OpenSSL	130
curl	120
OpenSSL	110
curl	100
OpenSSL	90
curl	80
OpenSSL	70
curl	60
OpenSSL	50
curl	40
OpenSSL	30
curl	20
OpenSSL	10
curl	10

Vulnerability Search... [+] [?] [≡]

Actions (0) ▼ Asset Vulnerability Group by ... ▼ Filters ▼ 1 - 200 of 2410 [<] [>] [Download] [Refresh] [Settings]

QID	TITLE	SEVERITY	LAST DETECTED	FIRST DETECTED	ASSET
105936	OpenSSH Command Injection Vulnerability (Generic) Active	Low	Oct 11, 2021	Mar 20, 2021	ip-172-31-7-120... 324815310
352851	Amazon Linux Security Advisory for ca-certificates: ALAS2-2021-1710 Active	Critical	Oct 11, 2021	Oct 06, 2021	ip-172-31-7-120... 324815310
352836	Amazon Linux Security Advisory for openldap: ALAS2-2021-1707 Active	Critical	Oct 11, 2021	Sep 21, 2021	ip-172-31-7-120... 324815310
352839	Amazon Linux Security Advisory for kernel: ALAS2-2021-1704 Active	Critical	Oct 11, 2021	Sep 21, 2021	ip-172-31-7-120... 324815310
352840	Amazon Linux Security Advisory for glibc: ALAS2-2021-1703 Active	Critical	Oct 11, 2021	Sep 21, 2021	ip-172-31-7-120... 324815310
352843	Amazon Linux Security Advisory for curl: ALAS2-2021-1700 Active	Critical	Oct 11, 2021	Sep 21, 2021	ip-172-31-7-120... 324815310
352799	Amazon Linux Security Advisory for kernel: ALAS2-2021-1699 Active	Critical	Oct 11, 2021	Sep 13, 2021	ip-172-31-7-120... 324815310
352506	Amazon Linux Security Advisory for curl: ALAS2-2021-1693 Active	Critical	Oct 11, 2021	Aug 12, 2021	ip-172-31-7-120... 324815310
352503	Amazon Linux Security Advisory for kernel: ALAS2-2021-1696 Active	Critical	Oct 11, 2021	Aug 12, 2021	ip-172-31-7-120... 324815310
352500	Amazon Linux Security Advisory for kernel: ALAS2-2021-1691 Active	Critical	Oct 11, 2021	Jul 29, 2021	ip-172-31-7-120... 324815310
352495	Amazon Linux Security Advisory for rpm: ALAS2-2021-1690 Active	Critical	Oct 11, 2021	Jul 21, 2021	ip-172-31-7-120... 324815310



007 - Vulnerability Findings



You can quickly and easily filter vulnerability findings by Severity Level, Category, Operating System, Detection Type and more.

The screenshot shows the Qualys Cloud Platform interface for managing vulnerability findings. On the left, there's a sidebar with a summary of '2.41K Total Detections' and dropdown menus for Severity, Category, Operating System, and Type Detected. A red box highlights the 'SEVERITY' dropdown menu. The main area is titled 'Vulnerabilities' and displays a list of findings. The first few rows of the table are:

ID	Title	Severity	Last Detected	First Detected	Asset
105936	OpenSSH Command Injection Vulnerability (Generic) Active	High	Oct 11, 2021	Mar 20, 2021	ip-172-31-7-120... 324815310
352851	Amazon Linux Security Advisory for ca-certificates: ALAS2-2021-1710 Active	Medium	Oct 11, 2021	Oct 06, 2021	ip-172-31-7-120... 324815310
352836	Amazon Linux Security Advisory for openldap: ALAS2-2021-1707 Active	Medium	Oct 11, 2021	Sep 21, 2021	ip-172-31-7-120... 324815310
352839	Amazon Linux Security Advisory for kernel: ALAS2-2021-1704 Active	Medium	Oct 11, 2021	Sep 21, 2021	ip-172-31-7-120... 324815310
352840	Amazon Linux Security Advisory for glibc: ALAS2-2021-1703 Active	Medium	Oct 11, 2021	Sep 21, 2021	ip-172-31-7-120... 324815310
352843	Amazon Linux Security Advisory for curl: ALAS2-2021-1700 Active	Medium	Oct 11, 2021	Sep 21, 2021	ip-172-31-7-120... 324815310
352799	Amazon Linux Security Advisory for kernel: ALAS2-2021-1699 Active	Medium	Oct 11, 2021	Sep 13, 2021	ip-172-31-7-120... 324815310
352506	Amazon Linux Security Advisory for curl: ALAS2-2021-1693 Active	Medium	Oct 11, 2021	Aug 12, 2021	ip-172-31-7-120... 324815310
352503	Amazon Linux Security Advisory for kernel: ALAS2-2021-1696 Active	Medium	Oct 11, 2021	Aug 12, 2021	ip-172-31-7-120... 324815310
352500	Amazon Linux Security Advisory for kernel: ALAS2-2021-1691 Active	Medium	Oct 11, 2021	Jul 29, 2021	ip-172-31-7-120... 324815310



007 - Vulnerability Findings

- ⓘ Let's narrow the scope of this list. In the "Search" field (near the top) we'll execute a query to list only patchable vulnerabilities...

Screenshot of the Qualys Cloud Platform Vulnerabilities page.

The page shows a total of 2.41K Total Detections. The left sidebar provides filters for Severity (4, 3, 5, 2, 1), Category (OEL, Windows, Local, CentOS, Internet Explorer, 11 more), Operating System (Oracle Enterprise..., Windows Server..., CentOS 6.5, Windows 10 Pro..., x86_64 Linux/2.6..., 11 more), and Type Detected (General, OS, Network, Application, Container).

The main table lists vulnerabilities:

ID	Title	Severity	Last Detected	First Detected	Asset
105936	OpenSSH Command Injection Vulnerability (Generic) Active	High	Oct 11, 2021	Mar 20, 2021	ip-172-31-7-120... 324815310
352851	Amazon Linux Security Advisory for ca-certificates: ALAS2-2021-1710 Active	Medium	Oct 11, 2021	Oct 06, 2021	ip-172-31-7-120... 324815310
352836	Amazon Linux Security Advisory for openldap: ALAS2-2021-1707 Active	Medium	Oct 11, 2021	Sep 21, 2021	ip-172-31-7-120... 324815310
352839	Amazon Linux Security Advisory for kernel: ALAS2-2021-1704 Active	Medium	Oct 11, 2021	Sep 21, 2021	ip-172-31-7-120... 324815310
352840	Amazon Linux Security Advisory for glibc: ALAS2-2021-1703 Active	Medium	Oct 11, 2021	Sep 21, 2021	ip-172-31-7-120... 324815310
352843	Amazon Linux Security Advisory for curl: ALAS2-2021-1700 Active	Medium	Oct 11, 2021	Sep 21, 2021	ip-172-31-7-120... 324815310
352799	Amazon Linux Security Advisory for kernel: ALAS2-2021-1699 Active	Medium	Oct 11, 2021	Sep 13, 2021	ip-172-31-7-120... 324815310
352506	Amazon Linux Security Advisory for curl: ALAS2-2021-1693 Active	Medium	Oct 11, 2021	Aug 12, 2021	ip-172-31-7-120... 324815310
352503	Amazon Linux Security Advisory for kernel: ALAS2-2021-1696 Active	Medium	Oct 11, 2021	Aug 12, 2021	ip-172-31-7-120... 324815310
352500	Amazon Linux Security Advisory for kernel: ALAS2-2021-1691 Active	Medium	Oct 11, 2021	Jul 29, 2021	ip-172-31-7-120... 324815310



007 - Vulnerability Findings



...and then execute to see the results.

Qualys Cloud Platform

VMDR ▾ DASHBOARD VULNERABILITIES PRIORITIZATION SCANS REPORTS REMEDIATION ASSETS KNOWLEDGEBASE USERS

Vulnerabilities

2.41K Total Detections

SEVERITY

Severity	Total Detections
4	954
3	945
5	314
2	181
1	16

CATEGORY

Category	Total Detections
OEL	691
Windows	630
Local	362
CentOS	278
Internet Explorer	203
11 more ▾	

OPERATING SYSTEM

Operating System	Total Detections
Oracle Enterprise...	438
Windows Server ...	437
CentOS 6.5	397
Windows 10 Pro ...	372
x86_64 Linux/2.6...	266
11 more ▾	

TYPE DETECTED

Type Detected	Total Detections
OpenSSH Command Injec...	954
Amazon Linux Security Advisory for ca-certificates: ALAS2-2021-1710	314
Amazon Linux Security Advisory for openldap: ALAS2-2021-1707	181
Amazon Linux Security Advisory for kernel: ALAS2-2021-1704	16
Amazon Linux Security Advisory for glibc: ALAS2-2021-1703	16
Amazon Linux Security Advisory for curl: ALAS2-2021-1700	16
Amazon Linux Security Advisory for kernel: ALAS2-2021-1699	16
Amazon Linux Security Advisory for curl: ALAS2-2021-1693	16
Amazon Linux Security Advisory for kernel: ALAS2-2021-1696	16
Amazon Linux Security Advisory for kernel: ALAS2-2021-1691	16
Amazon Linux Security Advisory for curl: ALAS2-2021-1680	16

Vulnerability ▾ [+] [?] [≡]

Actions (0) ▾ Asset Vulnerability Group by ... ▾ Filters ▾ 1 - 200 of 2410 [refresh] [down] [left] [right] [up] [gear]

QID	Title	Severity	Last Detected	First Detected	Asset
105936	OpenSSH Command Injection Vulnerability (Generic) Active	High	Oct 11, 2021	Mar 20, 2021	ip-172-31-7-120... 324815310
352851	Amazon Linux Security Advisory for ca-certificates: ALAS2-2021-1710 Active	High	Oct 11, 2021	Oct 06, 2021	ip-172-31-7-120... 324815310
352836	Amazon Linux Security Advisory for openldap: ALAS2-2021-1707 Active	High	Oct 11, 2021	Sep 21, 2021	ip-172-31-7-120... 324815310
352839	Amazon Linux Security Advisory for kernel: ALAS2-2021-1704 Active	High	Oct 11, 2021	Sep 21, 2021	ip-172-31-7-120... 324815310
352840	Amazon Linux Security Advisory for glibc: ALAS2-2021-1703 Active	High	Oct 11, 2021	Sep 21, 2021	ip-172-31-7-120... 324815310
352843	Amazon Linux Security Advisory for curl: ALAS2-2021-1700 Active	High	Oct 11, 2021	Sep 21, 2021	ip-172-31-7-120... 324815310
352799	Amazon Linux Security Advisory for kernel: ALAS2-2021-1699 Active	High	Oct 11, 2021	Sep 13, 2021	ip-172-31-7-120... 324815310
352506	Amazon Linux Security Advisory for curl: ALAS2-2021-1693 Active	High	Oct 11, 2021	Aug 12, 2021	ip-172-31-7-120... 324815310
352503	Amazon Linux Security Advisory for kernel: ALAS2-2021-1696 Active	High	Oct 11, 2021	Aug 12, 2021	ip-172-31-7-120... 324815310
352500	Amazon Linux Security Advisory for kernel: ALAS2-2021-1691 Active	High	Oct 11, 2021	Jul 29, 2021	ip-172-31-7-120... 324815310
352485	Amazon Linux Security Advisory for curl: ALAS2-2021-1680	High	Oct 11, 2021	Jul 05, 2021	ip-172-31-7-120... 324815310



007 - Vulnerability Findings



The result set now displays patchable vulnerabilities (those that have a patch in the Qualys Patch Catalog).

The screenshot shows the Qualys Cloud Platform interface. The top navigation bar includes links for VMDR, DASHBOARD, VULNERABILITIES (which is highlighted), PRIORITIZATION, SCANS, REPORTS, REMEDIATION, ASSETS, KNOWLEDGEBASE, and USERS. The user profile icon is in the top right corner.

The main content area has a blue header bar with the title "Vulnerabilities". On the left, there's a sidebar with summary statistics: "931 Total Detections", "SEVERITY" counts (4: 573, 5: 226, 3: 127, 2: 5), "CATEGORY" counts (Windows: 529, Internet Explorer: 200, CentOS: 113, Local: 61, RedHat: 20), "OPERATING SYSTEM" counts (Windows Server ...: 386, Windows 10 Pro ...: 304, CentOS 6.5: 69, Microsoft Windo...: 58, CentOS 6.4: 44, and a "6 more" link), and "TYPE DETECTED" counts (Confirmed: 927, Potential: 4). A large "Actions (0)" button is also present in the sidebar.

The main table lists 931 vulnerabilities. The columns are: ID, TITLE, SEVERITY, LAST DETECTED, FIRST DETECTED, and ASSET. Each row contains a link to the specific vulnerability details. The first few rows show Red Hat updates for microcode_ctl, sssd, dhcp, virt:rhel, and cloud-init. The last row is partially visible.

ID	TITLE	SEVERITY	LAST DETECTED	FIRST DETECTED	ASSET
239405	Red Hat Update for microcode_ctl (RHSA-2021:2308) Active	■■■■■	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239565	Red Hat Update for sssd (RHSA-2021:3151) Active	■■■■■	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239391	Red Hat Update for dhcp (RHSA-2021:2359) Active	■■■■■	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239539	Red Hat Update for virt:rhel and virt-devel:rhel (RHSA-2021:3061) Active	■■■■■	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239544	Red Hat Update for cloud-init (RHSA-2021:3081) Active	■■■■■	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239467	Red Hat Update for kernel (RHSA-2021:2570) Active	■■■■■	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239466	Red Hat Update for rpm (RHSA-2021:2574) Active	■■■■■	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239379	Red Hat Update for kernel (RHSA-2021:2168) Active	■■■■■	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239378	Red Hat Update for glib2 (RHSA-2021:2170) Active	■■■■■	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239363	Red Hat Update for polkit (RHSA-2021:2238) Active	■■■■■	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239455	Red Hat Update for libtiff (RHSA-2021:2678)	■■■■■	Oct 11, 2021	Sep 21, 2021	RHEL 8.4



007 - Vulnerability Findings

- ⓘ To receive patches, hosts must be running the Qualys Cloud Agent with the Patch Management module activated. We'll add these two requirements to our query.



007 - Vulnerability Findings

 Click the "Add" button.

Qualys Cloud Platform

VMDR DASHBOARD VULNERABILITIES PRIORITIZATION SCANS REPORTS REMEDIATION ASSETS KNOWLEDGEBASE USERS

Vulnerabilities

931 Total Detections

SEVERITY

4	573
5	226
3	127
2	5

CATEGORY

Windows	529
Internet Explorer	200
CentOS	113
Local	61
RedHat	20

OPERATING SYSTEM

Windows Server ...	386
Windows 10 Pro ...	304
CentOS 6.5	69
Microsoft Windo...	58
CentOS 6.4	44
6 more	4

TYPE DETECTED

Confirmed	927
Potential	4

Vulnerability vulnerabilities.vulnerability.qualysPatchable:TRUE

Actions (0) Asset Vulnerability Group by ... Filters 1 - 200 of 931

QID	TITLE	SEVERITY	LAST DETECTED	FIRST DETECTED	ASSET
239405	Red Hat Update for microcode_ctl (RHSA-2021:2308) <i>Active</i>	<div style="width: 80%;">██████</div>	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239565	Red Hat Update for sssd (RHSA-2021:3151) <i>Active</i>	<div style="width: 80%;">██████</div>	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239391	Red Hat Update for dhcp (RHSA-2021:2359) <i>Active</i>	<div style="width: 80%;">██████</div>	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239539	Red Hat Update for virt:rhel and virt-devel:rhel (RHSA-2021:3061) <i>Active</i>	<div style="width: 80%;">██████</div>	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239544	Red Hat Update for cloud-init (RHSA-2021:3081) <i>Active</i>	<div style="width: 80%;">██████</div>	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239467	Red Hat Update for kernel (RHSA-2021:2570) <i>Active</i>	<div style="width: 80%;">██████</div>	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239466	Red Hat Update for rpm (RHSA-2021:2574) <i>Active</i>	<div style="width: 80%;">██████</div>	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239379	Red Hat Update for kernel (RHSA-2021:2168) <i>Active</i>	<div style="width: 80%;">██████</div>	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239378	Red Hat Update for glib2 (RHSA-2021:2170) <i>Active</i>	<div style="width: 80%;">██████</div>	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239363	Red Hat Update for polkit (RHSA-2021:2238) <i>Active</i>	<div style="width: 80%;">██████</div>	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239465	Red Hat Update for lib4 (RHSA-2021:2675)	<div style="width: 80%;">██████</div>	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561



007 - Vulnerability Findings

- i A second "Search" field is added. We'll now include the "Cloud Agent Host" condition.

Qualys Cloud Platform

VMDR **VULNERABILITIES** **Prioritization** **SCANS** **REPORTS** **REMEDIATION** **ASSETS** **KNOWLEDGEBASE** **USERS**

Vulnerabilities

931 Total Detections

Severity	Count
4	573
5	226
3	127
2	5

Category	Count
Windows	529
Internet Explorer	200
CentOS	113
Local	61
RedHat	20

Operating System	Count
Windows Server ...	386
Windows 10 Pro ...	304
CentOS 6.5	69
Microsoft Windo...	58
CentOS 6.4	44
6 more	▼

Type Detected	Count
Confirmed	927
Potential	4

Vulnerability (?)

Asset (?)

Actions (0) ▼ Asset Vulnerability Group by ... Filters (?)

1 - 200 of 931 (?) (X) (<) (>) (refresh) (gear)

QID	Title	Severity	Last Detected	First Detected	Asset
239405	Red Hat Update for microcode_ctl (RHSA-2021:2308) Active	██████	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239565	Red Hat Update for sssd (RHSA-2021:3151) Active	██████	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239391	Red Hat Update for dhcp (RHSA-2021:2359) Active	██████	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239539	Red Hat Update for virt:rhel and virt-devel:rhel (RHSA-2021:3061) Active	██████	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239544	Red Hat Update for cloud-init (RHSA-2021:3081) Active	██████	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239467	Red Hat Update for kernel (RHSA-2021:2570) Active	██████	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239466	Red Hat Update for rpm (RHSA-2021:2574) Active	██████	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239379	Red Hat Update for kernel (RHSA-2021:2168) Active	██████	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239378	Red Hat Update for glib2 (RHSA-2021:2170) Active	██████	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239363	Red Hat Update for polkit (RHSA-2021:2238)	██████	Oct 11, 2021	Sep 21, 2021	RHEL 8.4



007 - Vulnerability Findings



The tags.name token set to the value of 'Cloud Agent' will include all agent hosts.

The screenshot shows the Qualys Cloud Platform interface under the 'VULNERABILITIES' tab. A search bar at the top contains two filters: 'vulnerabilities.vulnerability.qualysPatchable:TRUE' and 'tags.name: 'Cloud Agent''. The second filter is highlighted with a red box. On the left, there are summary sections for SEVERITY (4: 573, 5: 226, 3: 127, 2: 5), CATEGORY (Windows: 529, Internet Explorer: 200, CentOS: 113, Local: 61, RedHat: 20), OPERATING SYSTEM (Windows Server ...: 386, Windows 10 Pro ...: 304, CentOS 6.5: 69, Microsoft Windo...: 58, CentOS 6.4: 44, 6 more ...), and TYPE DETECTED (Confirmed: 927, Potential: 4). The main table lists 14 vulnerabilities, each with a QID, title, severity (4 stars), last detected date (Oct 11, 2021), first detected date (Sep 21, 2021), and asset (RHEL 8.4, 407550561).

QID	TITLE	SEVERITY	LAST DETECTED	FIRST DETECTED	ASSET
239405	Red Hat Update for microcode_ctl (RHSA-2021:2308) Active	4	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239565	Red Hat Update for sssd (RHSA-2021:3151) Active	4	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239391	Red Hat Update for dhcp (RHSA-2021:2359) Active	4	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239539	Red Hat Update for virt:rhel and virt-devel:rhel (RHSA-2021:3061) Active	4	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239544	Red Hat Update for cloud-init (RHSA-2021:3081) Active	4	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239467	Red Hat Update for kernel (RHSA-2021:2570) Active	4	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239466	Red Hat Update for rpm (RHSA-2021:2574) Active	4	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239379	Red Hat Update for kernel (RHSA-2021:2168) Active	4	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239378	Red Hat Update for glib2 (RHSA-2021:2170) Active	4	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239363	Red Hat Update for polkit (RHSA-2021:2238)	4	Oct 11, 2021	Sep 21, 2021	RHEL 8.4



007 - Vulnerability Findings

i We'll now add the "Activated Patch Management Module" condition.

Vulnerabilities

931 Total Detections

SEVERITY

Severity	Count
4	573
5	226
3	127
2	5

CATEGORY

Category	Count
Windows	529
Internet Explorer	200
CentOS	113
Local	61
RedHat	20

OPERATING SYSTEM

Operating System	Count
Windows Server ...	386
Windows 10 Pro ...	304
CentOS 6.5	69
Microsoft Windo...	58
CentOS 6.4	44
6 more	6

TYPE DETECTED

Type Detected	Count
Confirmed	927
Potential	4

Vulnerability

Asset

1 - 200 of 931

QID	Title	Severity	Last Detected	First Detected	Asset
239405	Red Hat Update for microcode_ctl (RHSA-2021:2308) <i>Active</i>	4	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239565	Red Hat Update for sssd (RHSA-2021:3151) <i>Active</i>	4	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239391	Red Hat Update for dhcp (RHSA-2021:2359) <i>Active</i>	4	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239539	Red Hat Update for virt:rhel and virt-devel:rhel (RHSA-2021:3061) <i>Active</i>	4	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239544	Red Hat Update for cloud-init (RHSA-2021:3081) <i>Active</i>	4	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239467	Red Hat Update for kernel (RHSA-2021:2570) <i>Active</i>	4	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239466	Red Hat Update for rpm (RHSA-2021:2574) <i>Active</i>	4	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239379	Red Hat Update for kernel (RHSA-2021:2168) <i>Active</i>	4	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239378	Red Hat Update for glib2 (RHSA-2021:2170) <i>Active</i>	4	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239363	Red Hat Update for polkit (RHSA-2021:2238)	4	Oct 11, 2021	Sep 21, 2021	RHEL 8.4



007 - Vulnerability Findings



Only agent hosts with the Patch Management module activated, will be included. Qualys Patch Management relies on Qualys Cloud Agents to provide the patching response.

The screenshot shows the Qualys Cloud Platform interface. The top navigation bar includes links for VMDR, DASHBOARD, VULNERABILITIES (which is selected), PRIORITIZATION, SCANS, REPORTS, REMEDIATION, ASSETS, KNOWLEDGEBASE, and USERS. The user profile icon is in the top right corner.

The main content area has a blue header bar with the title "Vulnerabilities". On the left, there's a sidebar with a summary: "931 Total Detections". Below this are sections for SEVERITY (4: 573, 5: 226, 3: 127, 2: 5) and CATEGORY (Windows: 529, Internet Explorer: 200, CentOS: 113, Local: 61, RedHat: 20). There's also a section for OPERATING SYSTEM (Windows Server ...: 386, Windows 10 Pro ...: 304, CentOS 6.5: 69, Microsoft Windo...: 58, CentOS 6.4: 44, 6 more ...), and a TYPE DETECTED section (Confirmed: 927, Potential: 4).

The central part of the screen displays a table of vulnerabilities. The table has columns: QID, TITLE, SEVERITY, LAST DETECTED, FIRST DETECTED, and ASSET. The first few rows show:

QID	TITLE	SEVERITY	LAST DETECTED	FIRST DETECTED	ASSET
239405	Red Hat Update for microcode_ctl (RHSA-2021:2308) Active	■■■■■	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239565	Red Hat Update for sssd (RHSA-2021:3151) Active	■■■■■	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239391	Red Hat Update for dhcp (RHSA-2021:2359) Active	■■■■■	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239539	Red Hat Update for virt:rhel and virt-devel:rhel (RHSA-2021:3061) Active	■■■■■	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239544	Red Hat Update for cloud-init (RHSA-2021:3081) Active	■■■■■	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239467	Red Hat Update for kernel (RHSA-2021:2570) Active	■■■■■	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239466	Red Hat Update for rpm (RHSA-2021:2574) Active	■■■■■	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239379	Red Hat Update for kernel (RHSA-2021:2168) Active	■■■■■	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239378	Red Hat Update for glib2 (RHSA-2021:2170) Active	■■■■■	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239363	Red Hat Update for polkit (RHSA-2021:2238)	■■■■■	Oct 11, 2021	Sep 21, 2021	RHEL 8.4



- ⓘ In its entirety, the query is looking for patchable vulnerabilities, discovered on host running the Qualys Cloud Agent with the Patch Management module activated. We'll execute this query to see the new result.



007 - Vulnerability Findings

Qualys Cloud Platform

VMDR ▾ DASHBOARD VULNERABILITIES PRIORITIZATION SCANS REPORTS REMEDIATION ASSETS KNOWLEDGEBASE USERS

Vulnerabilities

931 Total Detections

Vulnerability Asset

931 Total Detections

SEVERITY

4	573
5	226
3	127
2	5

CATEGORY

Windows	529
Internet Explorer	200
CentOS	113
Local	61
RedHat	20

OPERATING SYSTEM

Windows Server ...	386
Windows 10 Pro ...	304
CentOS 6.5	69
Microsoft Windo...	58
CentOS 6.4	44
6 more ▾	

TYPE DETECTED

Confirmed	927
Potential	4

1 - 200 of 931

QID	TITLE	SEVERITY	LAST DETECTED	FIRST DETECTED	ASSET
239405	Red Hat Update for microcode_ctl (RHSA-2021:2308) Active	■■■■■	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239565	Red Hat Update for sssd (RHSA-2021:3151) Active	■■■■■	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239391	Red Hat Update for dhcp (RHSA-2021:2359) Active	■■■■■	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239539	Red Hat Update for virt:rhel and virt-devel:rhel (RHSA-2021:3061) Active	■■■■■	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239544	Red Hat Update for cloud-init (RHSA-2021:3081) Active	■■■■■	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239467	Red Hat Update for kernel (RHSA-2021:2570) Active	■■■■■	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239466	Red Hat Update for rpm (RHSA-2021:2574) Active	■■■■■	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239379	Red Hat Update for kernel (RHSA-2021:2168) Active	■■■■■	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239378	Red Hat Update for glib2 (RHSA-2021:2170) Active	■■■■■	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239363	Red Hat Update for polkit (RHSA-2021:2238)	■■■■■	Oct 11, 2021	Sep 21, 2021	RHEL 8.4



007 - Vulnerability Findings



The result set now lists vulnerabilities that can be successfully patched with Qualys VMDR. Click the **check box** at the top of the list (just below the "Search" fields).

Screenshot of the Qualys Cloud Platform VMDR interface showing a list of vulnerabilities.

Vulnerabilities (123 Total Detections)

FILTERS:

- Vulnerability: `vulnerabilities.vulnerability.qualysPatchable:TRUE`
- Asset: `tags.name:'Cloud Agent' and activatedForModules:PM`

Actions (0) Asset Vulnerability Group by ... Filters

QID	TITLE	SEVERITY	LAST DETECTED	FIRST DETECTED	ASSET
239405	Red Hat Update for microcode_ctl (RHSA-2021:2308) <i>Active</i>	■■■■■	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239565	Red Hat Update for sssd (RHSA-2021:3151) <i>Active</i>	■■■■■	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239391	Red Hat Update for dhcp (RHSA-2021:2359) <i>Active</i>	■■■■■	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239539	Red Hat Update for virt:rhel and virt-devel:rhel (RHSA-2021:3061) <i>Active</i>	■■■■■	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239544	Red Hat Update for cloud-init (RHSA-2021:3081) <i>Active</i>	■■■■■	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239467	Red Hat Update for kernel (RHSA-2021:2570) <i>Active</i>	■■■■■	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239466	Red Hat Update for rpm (RHSA-2021:2574) <i>Active</i>	■■■■■	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239379	Red Hat Update for kernel (RHSA-2021:2168) <i>Active</i>	■■■■■	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239378	Red Hat Update for glib2 (RHSA-2021:2170) <i>Active</i>	■■■■■	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239363	Red Hat Update for polkit (RHSA-2021:2238)	■■■■■	Oct 11, 2021	Sep 21, 2021	RHEL 8.4



007 - Vulnerability Findings

 With all vulnerabilities selected, click the "Actions" button...

Qualys Cloud Platform

VMDR **VULNERABILITIES** **Prioritization** **SCANS** **REPORTS** **REMEDIATION** **ASSETS** **KNOWLEDGEBASE** **USERS**

Vulnerabilities

123 Total Detections

SEVERITY

4	68
3	33
5	22

CATEGORY

Windows	59
Local	30
RedHat	20
Internet Explorer	14

OPERATING SYSTEM

Microsoft Windo...	58
Microsoft Windo...	18
Red Hat Enterpris...	17
Microsoft Windo...	14
Microsoft Windo...	13
1 more	1

TYPE DETECTED

Confirmed	123
-----------	-----

STATUS

ACTIVE	122
--------	-----

Vulnerability **Asset**

Actions (123) **Asset** **Vulnerability** **Group by ...** **Filters**

1 - 123 of 123

QID	TITLE	SEVERITY	LAST DETECTED	FIRST DETECTED	ASSET
239405	Red Hat Update for microcode_ctl (RHSA-2021:2308) Active	██████	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239565	Red Hat Update for sssd (RHSA-2021:3151) Active	██████	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239391	Red Hat Update for dhcp (RHSA-2021:2359) Active	██████	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239539	Red Hat Update for virt:rhel and virt-devel:rhel (RHSA-2021:3061) Active	██████	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239544	Red Hat Update for cloud-init (RHSA-2021:3081) Active	██████	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239467	Red Hat Update for kernel (RHSA-2021:2570) Active	██████	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239466	Red Hat Update for rpm (RHSA-2021:2574) Active	██████	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239379	Red Hat Update for kernel (RHSA-2021:2168) Active	██████	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239378	Red Hat Update for glib2 (RHSA-2021:2170) Active	██████	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239363	Red Hat Update for polkit (RHSA-2021:2238) Active	██████	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561



007 - Vulnerability Findings



...and select View Missing Patches.

The screenshot shows the Qualys Cloud Platform interface for vulnerability management. The top navigation bar includes links for VMDR, DASHBOARD, VULNERABILITIES (which is selected), PRIORITIZATION, SCANS, REPORTS, REMEDIATION, ASSETS, KNOWLEDGEBASE, and USERS. The user profile icon is in the top right corner.

The main content area is titled "Vulnerabilities". On the left, there's a summary box showing "123 Total Detections". Below it are three tables: "SEVERITY" (with counts for 4, 3, and 5), "CATEGORY" (Windows 59, Local 30, RedHat 20, Internet Explorer 14), and "OPERATING SYSTEM" (Microsoft Windows 58, Microsoft Windows 18, Red Hat Enterprise Linux 17, Microsoft Windows 14, Microsoft Windows 13, plus 1 more). The "TYPE DETECTED" section shows "Confirmed" with 123 detections. The "STATUS" section shows "ACTIVE" with 122 detections.

The central part of the screen displays a list of vulnerabilities. A search bar at the top allows filtering by "Vulnerability" (containing "vulnerabilities.vulnerability.qualysPatchable:TRUE") and "Asset" (containing "tags.name:'Cloud Agent' and activatedForModules:PM"). Below the search bar are buttons for "Actions (123)", "Asset", "Vulnerability", "Group by ...", and "Filters".

The main list table has columns for "ID", "Title", "Severity", "Last Detected", "First Detected", and "Asset". A "View Missing Patches" button is located above the first row of the table. The table lists 123 vulnerabilities, with the first few entries being:

ID	Title	Severity	Last Detected	First Detected	Asset
239405	Red Hat Update for microcode_ctl (RHSA-2021:2308) Active	Medium	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239565	Red Hat Update for sssd (RHSA-2021:3151) Active	Medium	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239391	Red Hat Update for dhcp (RHSA-2021:2359) Active	Medium	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239539	Red Hat Update for virt:rhel and virt-devel:rhel (RHSA-2021:3061) Active	Medium	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239544	Red Hat Update for cloud-init (RHSA-2021:3081) Active	Medium	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239467	Red Hat Update for kernel (RHSA-2021:2570) Active	Medium	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239466	Red Hat Update for rpm (RHSA-2021:2574) Active	Medium	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239379	Red Hat Update for kernel (RHSA-2021:2168) Active	Medium	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239378	Red Hat Update for glib2 (RHSA-2021:2170) Active	Medium	Oct 11, 2021	Sep 21, 2021	RHEL 8.4 407550561
239363	Red Hat Update for polkit (RHSA-2021:2238)	Medium	Oct 11, 2021	Sep 21, 2021	RHEL 8.4



007 - Vulnerability Findings

- i Patching is supported for both Linux and Windows hosts. For this example, click the "View Missing Patches" button for Linux.



007 - Vulnerability Findings

- ⓘ You are automatically placed within the Patch Catalog, of the Patch Management application and all patches for the selected vulnerabilities are now displayed. Click the **check box** at the top (just below the "Search" fields) to select all patches.



007 - Vulnerability Findings

Qualys Cloud Platform

Patch Management New Updates

DASHBOARD PATCHES ASSETS JOBS CONFIGURATION

Patch Catalog Windows Linux

20 Total Patches

PATCH TITLE PUBLISHED DATE ARCHIT ADVISORY ID CATEGORY QID VENDOR SEVERITY MISSING ASSETS

RHSA-2021:3327: kernel security and bug fix update	Aug 30, 2021	x86_6...	RHSA-2021:3327	Security	239603	Important	1	
RHSA-2021:3325: bind security update	Aug 30, 2021	-	x86_6...	RHSA-2021:3325	Security	239604	Moderate	1
RHSA-2021:3151: sssd security update	Aug 15, 2021	-	aarch...	RHSA-2021:3151	Security	239565	Important	1
RHSA-2021:3061: virt:rhel and virt-devel:rhel security and bug fix update	Aug 09, 2021	-	aarch...	RHSA-2021:3061	Security	239539	Moderate	1
RHSA-2021:3081: cloud-init security update	Aug 09, 2021	-	noarch	RHSA-2021:3081	Security	239544	Moderate	1
RHSA-2021:3057: kernel security, bug fix, and enhancement update	Aug 09, 2021	⌚	aarch...	RHSA-2021:3057	Security	239541	Important	1
RHSA-2021:3058: glib2 security update	Aug 09, 2021	-	aarch...	RHSA-2021:3058	Security	239540	Moderate	1
RHSA-2021:3027: microcode_ctl security, bug fix and enhancement update	Aug 08, 2021	-	x86_6...	RHSA-2021:3027	Security	239535	Important	1
RHSA-2021:2725: kernel security and bug fix update	Jul 20, 2021	⌚	x86_6...	RHSA-2021:2725	Security	239524	Important	1
RHSA-2021:2717: systemd security update	Jul 20, 2021	⌚	aarch...	RHSA-2021:2717	Security	239503	Important	1

Actions (0) Filters 1 - 20 of 20

OS: RHEL8 (17), RHEL7 (3)

VENDOR SEVERITY: Important (13), Moderate (7)



007 - Vulnerability Findings

- With all patches selected, click the "Actions" button.

The screenshot shows the Qualys Cloud Platform Patch Management interface. The top navigation bar includes links for Patch Management (selected), Dashboard, Patches (selected), Assets, Jobs, and Configuration, along with user icons. The main area is titled 'Patch Catalog' with tabs for Windows and Linux. A sidebar on the left displays statistics: 20 Total Patches, OS distribution (RHEL8: 17, RHEL7: 3), and Vendor Severity (Important: 13, Moderate: 7). The central table lists 10 vulnerabilities, each with a checkbox checked in the first column. The columns include Patch Title, Published Date, Archit, Advisory ID, Category, QID, Vendor Severity, and Missing Assets. The first vulnerability listed is 'RHSA-2021:3327: kernel security and bug fix update'.

PATCH TITLE	PUBLISHED DATE	ARCHIT	ADVISORY ID	CATEGORY	QID	VENDOR SEVERITY	MISSING ASSETS
RHSA-2021:3327: kernel security and bug fix update	Aug 30, 2021	x86_6...	RHSA-2021:3327	Security	239603	Important	1
RHSA-2021:3325: bind security update	Aug 30, 2021	-	x86_6...	RHSA-2021:3325	Security	Moderate	1
RHSA-2021:3151: sssd security update	Aug 15, 2021	-	aarch...	RHSA-2021:3151	Security	Important	1
RHSA-2021:3061: virt:rhel and virt-devel:rhel security and bug fix update	Aug 09, 2021	-	aarch...	RHSA-2021:3061	Security	Moderate	1
RHSA-2021:3081: cloud-init security update	Aug 09, 2021	-	noarch	RHSA-2021:3081	Security	Moderate	1
RHSA-2021:3057: kernel security, bug fix, and enhancement update	Aug 09, 2021	(empty)	aarch...	RHSA-2021:3057	Security	Important	1
RHSA-2021:3058: glib2 security update	Aug 09, 2021	-	aarch...	RHSA-2021:3058	Security	Moderate	1
RHSA-2021:3027: microcode_ctl security, bug fix and enhancement update	Aug 08, 2021	-	x86_6...	RHSA-2021:3027	Security	Important	1
RHSA-2021:2725: kernel security and bug fix update	Jul 20, 2021	(empty)	x86_6...	RHSA-2021:2725	Security	Important	1
RHSA-2021:2717: systemd security update	Jul 20, 2021	(empty)	aarch...	RHSA-2021:2717	Security	Important	1



007 - Vulnerability Findings



...and select Add to Existing Job.

The screenshot shows the Qualys Cloud Platform Patch Management interface. The top navigation bar includes links for Patch Management (selected), Dashboard, Patches (highlighted in blue), Assets, Jobs, and Configuration, along with user icons. The main area is titled 'Patch Catalog' with tabs for Windows and Linux. A sidebar on the left displays statistics: 20 Total Patches, OS distribution (RHEL8: 17, RHEL7: 3), and Vendor Severity (Important: 13, Moderate: 7). The central panel lists 20 vulnerabilities, each with a checkbox, an 'Actions' dropdown menu (containing 'View Details', 'Add to Existing Job' (which is highlighted in blue), 'Add to New Job', and 'Remove Patch'), and detailed information like Published Date, Archit, Advisory ID, Category, QID, Vendor Severity (with a color-coded box), and Missing Assets. The 'Add to Existing Job' option is clearly visible for each item in the list.

Action	Description	PUBLISHED DATE	ARCHIT	ADVISORY ID	CATEGORY	QID	VENDOR SEVERITY	MISSING ASSETS
Add to Existing Job	el security and bug fix update	Aug 30, 2021	x86_6...	RHSA-2021:3327	Security	239603	Important	1
Add to Existing Job	security update	Aug 30, 2021	-	x86_6...	RHSA-2021:3325	Security	Moderate	1
Add to Existing Job	RHSA-2021:3151: sssd security update	Aug 15, 2021	-	aarch...	RHSA-2021:3151	Security	Important	1
Add to Existing Job	RHSA-2021:3061: virt:rhel and virt-devel:rhel security and bug fix update	Aug 09, 2021	-	aarch...	RHSA-2021:3061	Security	Moderate	1
Add to Existing Job	RHSA-2021:3081: cloud-init security update	Aug 09, 2021	-	noarch	RHSA-2021:3081	Security	Moderate	1
Add to Existing Job	RHSA-2021:3057: kernel security, bug fix, and enhancement update	Aug 09, 2021	(empty)	aarch...	RHSA-2021:3057	Security	Important	1
Add to Existing Job	RHSA-2021:3058: glib2 security update	Aug 09, 2021	-	aarch...	RHSA-2021:3058	Security	Moderate	1
Add to Existing Job	RHSA-2021:3027: microcode_ctl security, bug fix and enhancement update	Aug 08, 2021	-	x86_6...	RHSA-2021:3027	Security	Important	1
Add to Existing Job	RHSA-2021:2725: kernel security and bug fix update	Jul 20, 2021	(empty)	x86_6...	RHSA-2021:2725	Security	Important	1
Add to Existing Job	RHSA-2021:2717: systemd security update	Jul 20, 2021	(empty)	aarch...	RHSA-2021:2717	Security	Important	1



007 - Vulnerability Findings

- ⓘ We'll add the patches to a patch deployment job that is scheduled to run daily. Select the **check box** for the **"Daily Patch Deployment"** job.

The screenshot shows the 'Add Patches: Existing Deployment Jobs' page in the Qualys Cloud Platform. On the left, there's a sidebar with summary statistics: 1 Total Job, 1 Enabled, 1 Daily, and 1 Install. The main area has a search bar and a message about asset counts. Below is a table with columns: STATUS, JOB NAME, OWNER, SCHEDULE, PATCHES, ASSETS, and TAGS. One job is listed:

STATUS	JOB NAME	OWNER	SCHEDULE	PATCHES	ASSETS	TAGS
Enabled	Daily Patch Deployment - Linux Install Job	quays2pn1 Oct 02, 2021	Daily, 12:00 am	0	2*	OS: Linux



007 - Vulnerability Findings

- ⓘ Click the "Add" button.

The screenshot shows the 'Add Patches: Existing Deployment Jobs' interface in Qualys Cloud Platform. On the left, a sidebar summary shows 1 Total Job, with breakdowns by STATUS (Enabled), SCHEDULED (Daily), and JOB TYPE (Install). The main area lists the single job:

STATUS	JOB NAME	OWNER	SCHEDULE	PATCHES	ASSETS	TAGS
Enabled	Daily Patch Deployment - Linux Install Job	quays2pn1 Oct 02, 2021	Daily, 12:00 am	0	2*	OS: Linux

At the top right, there are navigation icons for help, search, and settings. Below the table, there are links for '1 - 1 of 1' and various actions like refresh and settings.



007 - Vulnerability Findings

- ⓘ The selected patches have been successfully added to the Daily Patch Deployment job. They will be deployed the very next time this job is scheduled to run.

The screenshot shows the Qualys Cloud Platform interface for Patch Management. The top navigation bar includes links for Patch Management (selected), New Updates, Dashboard, Patches, Assets, JOBS (selected), and Configuration. A user icon with a question mark is also present. The main content area is titled 'Jobs' and has tabs for Windows and Linux. A sidebar on the left displays summary statistics: 1 Total Job, 1 Enabled, 1 SCHEDULED (Daily), and 1 JOB TYPE (Install). The main table lists one job: 'Daily Patch Deployment - Linux' (Install Job), which is Enabled, owned by 'quays2pn1', scheduled daily at 12:00 am on Oct 02, 2021, and contains 20 patches, 2 assets, and the tag 'OS: Linux'. A note indicates that the final number of assets will be calculated before the job starts. Action buttons include Actions (0), Create Job, and Filters.

Status	Name	Owner	Schedule	Patches	Assets	Tags
Enabled	Daily Patch Deployment - Linux Install Job	quays2pn1	Daily, 12:00 am Oct 02, 2021	20	2*	OS: Linux



007 - Vulnerability Findings

- ⓘ This concludes the "Vulnerability Findings" tutorial. Close this window and continue to read through your Lab Tutorial Supplement.

The screenshot shows the Qualys Cloud Platform interface for Patch Management. The top navigation bar includes links for Patch Management (with a dropdown for New Updates), DASHBOARD, PATCHES, ASSETS, JOBS (which is selected and highlighted in blue), and CONFIGURATION. On the far right are user icons for profile, help, and email.

The main content area is titled 'Jobs' and has tabs for Windows and Linux. A sidebar on the left displays summary statistics: 1 Total Job, 1 Enabled, 1 Daily SCHEDULED, and 1 Install JOB TYPE. The central table lists the single job:

STATUS	NAME	OWNER	SCHEDULE	PATCHES	ASSETS	TAGS
Enabled	Daily Patch Deployment - Linux Install Job	quays2pn1 Oct 02, 2021	Daily, 12:00 am	20	2*	OS: Linux

Below the table, there are buttons for Actions (0), Create Job, and Filters, along with pagination information (1 - 1 of 1) and various icons for filtering and sorting.



007 - Vulnerability Findings



Scan to go to the interactive player