

- i Understanding the Knowledgebase is an important, foundational subject which you need to know before you master other subjects. Can you see how many vulnerabilities are included in total? [Click anywhere to continue.](#)

Qualys Cloud Platform

VMDR

Dashboard Vulnerabilities Prioritization Scans Reports Remediation Assets KnowledgeBase Users

KnowledgeBase Predictions Search Lists

New Search

1 - 20 of 123122

QID	Title	Severity	Category	CVE ID	Vendor Reference	CVSS Base	CVSS3.1 Base	Bugtraq ID	Modified	Published
20362	IBM Db2 Privilege Escalation Vulnerability (7010571)		Database	CVE-2023-27558	7010571	7.2	7.8		08/29/2023	08/28/2023
378802	Wireshark CP2179 dissector crash Vulnerability (wnpa-sec-2023-26)		Local		wnpa-sec-2023-26	5.4	8.6		08/29/2023	08/28/2023
378803	Wireshark CBOR dissector crash Vulnerability (wnpa-sec-2023-23)		Local		wnpa-sec-2023-23	5.4	8.6		08/29/2023	08/28/2023
378800	Wireshark BT SDP dissector memory leak Vulnerability (wnpa-sec-2023-25)		Local		wnpa-sec-2023-25	5.4	8.6		08/29/2023	08/28/2023
378801	Wireshark BT SDP dissector infinite loop Vulnerability (wnpa-sec-2023-24)		Local		wnpa-sec-2023-24	5.4	8.6		08/29/2023	08/28/2023
691236	Free Berkeley Software Distribution (FreeBSD) Security Update for phpmyfaq (ddd3fcc9-2bdd-11ee-9af4-589cf0f81b0)		FreeBSD		ddd3fcc9-2bdd-11ee-9af4-589cf0f81b0	5.4	8.6		08/29/2023	08/28/2023
378810	Microsoft Edge Based on Chromium Prior to 116.0.1938.62 Multiple Vulnerabilities		Local	CVE-2023-4428, CVE-2023-36741, CVE-2023-4431, CVE-2023-4429 ...	Edge (chromium based)	5.4	8.8		08/29/2023	08/28/2023
503288	Alpine Linux Security Update for xen		Alpine Linux	CVE-2022-40982, CVE-2022-42331, CVE-2022-42332, CVE-2022-42333	xen	5.4	8.6		08/29/2023	08/28/2023
284441	Fedora Security Update for youtube (FEDORA-2023-1f11546a48)		Fedora	CVE-2023-35934	FEDORA-2023-1f11546a48	5.4	8.2		08/29/2023	08/28/2023
284440	Fedora Security Update for youtube (FEDORA-2023-5435c10480)		Fedora	CVE-2023-35934	FEDORA-2023-5435c10480	5.4	8.2		08/29/2023	08/28/2023
284446	Fedora Security Update for xen (FEDORA-2023-04473fc41e)		Fedora	CVE-2023-34320, CVE-2023-20569, CVE-2022-04473fc41e	FEDORA-2023-04473fc41e	5.4	7.5		08/29/2023	08/28/2023

-  The main list includes a summary of each vulnerability, including CVE and vendor references, the CVSS base score, and the publication date. Now click on the [Search button](#) to begin filtering this list.

VMDR										
KnowledgeBase										
KnowledgeBase		Predictions		Search Lists						
New		Search								
QID	Title	Severity	Category	CVE ID	Vendor Reference	CVSS Base	CVSS3.1 Base	Bugtraq ID	Modified	Published
20362	IBM Db2 Privilege Escalation Vulnerability (7010571)		Database	CVE-2023-27558	7010571	7.2	7.8		08/29/2023	08/28/2023
378802	Wireshark CP2179 dissector crash Vulnerability (wnpa-sec-2023-26)		Local		wnpa-sec-2023-26	5.4	8.6		08/29/2023	08/28/2023
378803	Wireshark CBOR dissector crash Vulnerability (wnpa-sec-2023-23)		Local		wnpa-sec-2023-23	5.4	8.6		08/29/2023	08/28/2023
378800	Wireshark BT SDP dissector memory leak Vulnerability (wnpa-sec-2023-25)		Local		wnpa-sec-2023-25	5.4	8.6		08/29/2023	08/28/2023
378801	Wireshark BT SDP dissector infinite loop Vulnerability (wnpa-sec-2023-24)		Local		wnpa-sec-2023-24	5.4	8.6		08/29/2023	08/28/2023
691236	Free Berkeley Software Distribution (FreeBSD) Security Update for phpmyfaq (ddd3ffcc9-2bdd-11ee-9af4-589cf0f81b0)		FreeBSD		ddd3ffcc9-2bdd-11ee-9af4-589cf0f81b0	5.4	8.6		08/29/2023	08/28/2023
378810	Microsoft Edge Based on Chromium Prior to 116.0.1938.62 Multiple Vulnerabilities		Local	CVE-2023-4428, CVE-2023-36741, CVE-2023-4431, CVE-2023-4429 ...	Edge (chromium based)	5.4	8.8		08/29/2023	08/28/2023
503288	Alpine Linux Security Update for xen		Alpine Linux	CVE-2022-40982, CVE-2022-42331, CVE-2022-42332, CVE-2022-42333	xen	5.4	8.6		08/29/2023	08/28/2023
284441	Fedora Security Update for youtube (FEDORA-2023-1f11546a48)		Fedora	CVE-2023-35934	FEDORA-2023-1f11546a48	5.4	8.2		08/29/2023	08/28/2023
284440	Fedora Security Update for youtube (FEDORA-2023-5435c10480)		Fedora	CVE-2023-35934	FEDORA-2023-5435c10480	5.4	8.2		08/29/2023	08/28/2023
284446	Fedora Security Update for xen (FEDORA-2023-04473fc41e)		Fedora	CVE-2023-34320, CVE-2023-20569, CVE-2022-04473fc41e	FEDORA-2023-04473fc41e	5.4	7.5		08/29/2023	08/28/2023

- In the Search dialog box, click on the scroll bar to scroll down.

The screenshot shows the Qualys Cloud Platform interface with the 'KnowledgeBase' tab selected. A search dialog box is open, containing various search filters like QID, Title, Discovery Method, Authentication Type, User Configuration, Category, Patch Solution, CVE ID, and CPE. Below the dialog, a table lists several security vulnerabilities, each with details such as QID, Title, Description, CVSS Score, FEDORA ID, and Last Modified date. The table includes entries for vulnerabilities like 'IBM Db2 Privilege Escalation Vulnerability' and 'Fedora Security Update for xen'.

QID	Title	Description	CVSS Score	FEDORA ID	Last Modified
20362	IBM Db2 Privilege Escalation Vulnerability (70)	Details	7.0	5435c10480	08/29/2023 08/28/2023
378800	Wireshark BT SDP dissector memory leak Vulnerability	Details	8.2	1ff11546a48	08/29/2023 08/28/2023
378803	Wireshark CBOR dissector crash Vulnerability	Details	8.2	1ff11546a48	08/29/2023 08/28/2023
378801	Wireshark BT SDP dissector infinite loop Vulnerability	Details	8.2	1ff11546a48	08/29/2023 08/28/2023
691236	Free Berkeley Software Distribution (FreeBSD) (ddd3fcc9-2bdd-11ee-9af4-5899cf0f81b0)	Details	8.2	1ff11546a48	08/29/2023 08/28/2023
378802	Wireshark CP2179 dissector crash Vulnerability	Details	8.2	1ff11546a48	08/29/2023 08/28/2023
378810	Microsoft Edge Based on Chromium Prior to 106.0.5240.22 Vulnerabilities	Details	8.2	1ff11546a48	08/29/2023 08/28/2023
503288	Alpine Linux Security Update for xen	Details	8.2	1ff11546a48	08/29/2023 08/28/2023
284440	Fedora Security Update for youtube (FEDORA-2023-04473fc41e)	Details	8.2	1ff11546a48	08/29/2023 08/28/2023
284441	Fedora Security Update for youtube (FEDORA-2023-1ff11546a48)	Details	8.2	1ff11546a48	08/29/2023 08/28/2023
284446	Fedora Security Update for xen (FEDORA-2023-04473fc41e)	Details	7.5	1ff11546a48	08/29/2023 08/28/2023

- 1 You are now going to filter the knowledgebase to only those entries published in the previous month. Click on the drop down arrow next to "Published".

The screenshot shows the Qualys Cloud Platform interface. The top navigation bar includes VMDR, Dashboard, Vulnerabilities, Prioritization, Scans, Reports, Remediation, Assets, KnowledgeBase (which is selected), and Users. A search bar at the top has the text "Qualys Cloud Platform". Below the navigation is a sub-navigation bar with KnowledgeBase, Predictions, and Search Lists. A modal window titled "Search" is open, containing various search filters: Bugtraq ID, Service Modified, User Modified, Published (with a dropdown menu showing "Select a date"), Confirmed Severity (radio buttons for Level 1 to Level 5), Potential Severity (radio buttons for Level 1 to Level 5), Information Severity (radio buttons for Level 1 to Level 5), Vendor (dropdown menu showing "All"), Product (dropdown menu showing "All"), and Vulnerability Details (text input field). At the bottom of the search dialog is a "Search" button. To the right of the search dialog is a table of search results. The table has columns: Bugtraq ID, Modified, and Published. The results show several entries from August 29, 2023, and August 28, 2023.

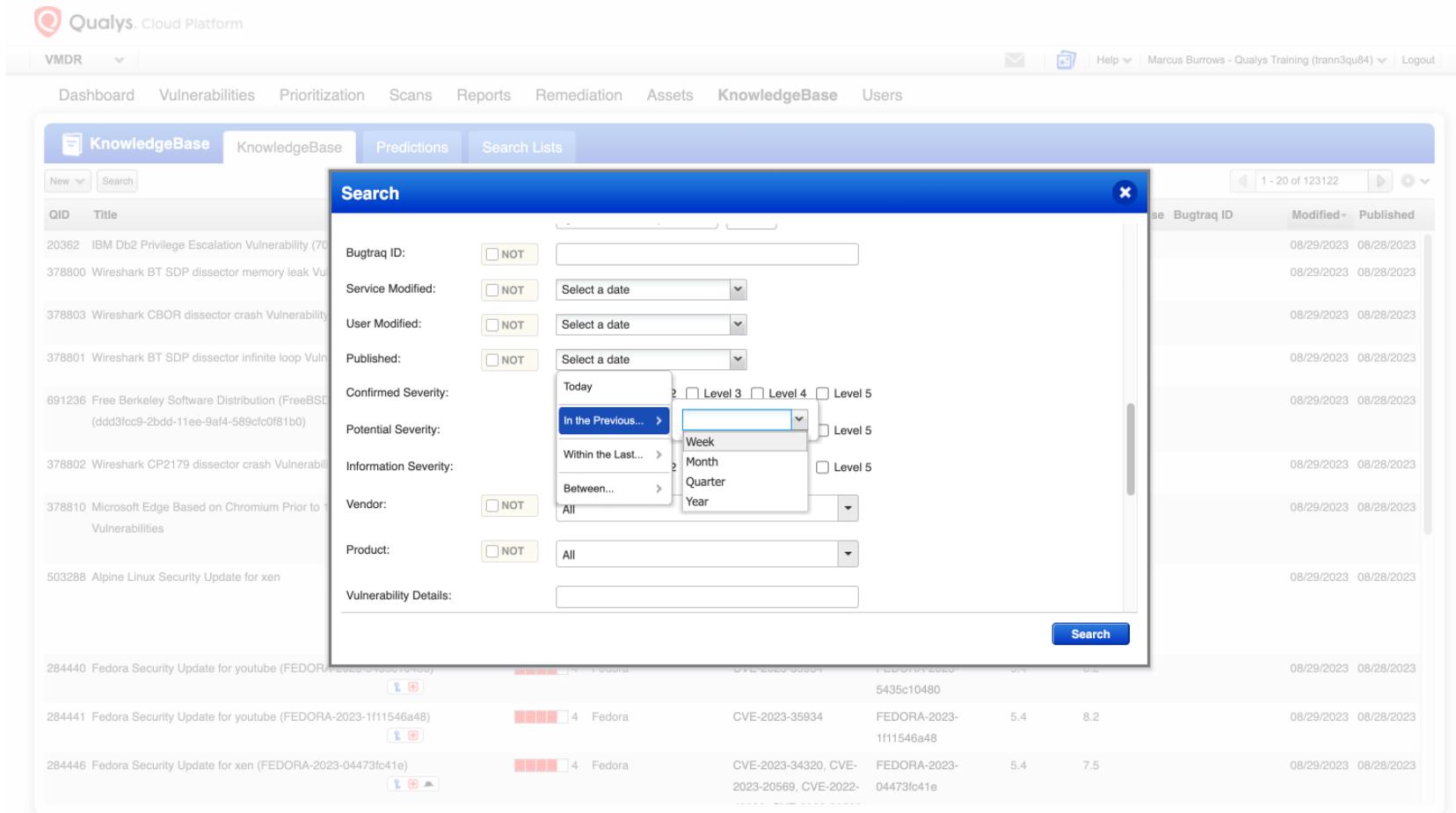
Bugtraq ID	Modified	Published
20362 IBM Db2 Privilege Escalation Vulnerability (70)	08/29/2023	08/28/2023
378800 Wireshark BT SDP dissector memory leak Vu	08/29/2023	08/28/2023
378803 Wireshark CBOR dissector crash Vulnerabilit	08/29/2023	08/28/2023
378801 Wireshark BT SDP dissector infinite loop Vu	08/29/2023	08/28/2023
691236 Free Berkeley Software Distribution (FreeBSD (ddd3fcc9-2bdd-11ee-9af4-589cf0f81b0)	08/29/2023	08/28/2023
378802 Wireshark CP2179 dissector crash Vulnerabilit	08/29/2023	08/28/2023
378810 Microsoft Edge Based on Chromium Prior to 1 Vulnerabilities	08/29/2023	08/28/2023
503288 Alpine Linux Security Update for xen	08/29/2023	08/28/2023
284440 Fedora Security Update for youtube (FEDORA-2023-34320, CVE-2023-35934)	08/29/2023	08/28/2023
284441 Fedora Security Update for youtube (FEDORA-2023-1ff11546a48)	08/29/2023	08/28/2023
284446 Fedora Security Update for xen (FEDORA-2023-04473fc41e)	08/29/2023	08/28/2023

1 Click the drop down arrow to select a time range.

The screenshot shows the Qualys Cloud Platform interface, specifically the KnowledgeBase section. A search dialog box is open over a list of vulnerabilities. The search dialog includes fields for QID, Title, Bugtraq ID, Service Modified, User Modified, Published (with a dropdown menu open), Confirmed Severity, Potential Severity, Information Severity, Vendor, Product, and Vulnerability Details. The 'Published' dropdown menu is highlighted, showing options like 'Today', 'In the Previous...', 'Within the Last...', 'Between...', and 'All'. The main table lists vulnerabilities with columns for QID, Title, Bugtraq ID, Modified, Published, and several other details. The 'Published' column shows dates like 08/29/2023 and 08/28/2023.

QID	Title	Bugtraq ID	Modified	Published			
20362	IBM Db2 Privilege Escalation Vulnerability (70)		08/29/2023	08/28/2023			
378800	Wireshark BT SDP dissector memory leak Vulnerability		08/29/2023	08/28/2023			
378803	Wireshark CBOR dissector crash Vulnerability		08/29/2023	08/28/2023			
378801	Wireshark BT SDP dissector infinite loop Vulnerability		08/29/2023	08/28/2023			
691236	Free Berkeley Software Distribution (FreeBSD) (ddd3fcc9-2bdd-11ee-9af4-589fcf0f81b0)		08/29/2023	08/28/2023			
378802	Wireshark CP2179 dissector crash Vulnerability		08/29/2023	08/28/2023			
378810	Microsoft Edge Based on Chromium Prior to 106.0.5249.62 Vulnerabilities		08/29/2023	08/28/2023			
503288	Alpine Linux Security Update for xen		08/29/2023	08/28/2023			
284440	Fedora Security Update for youtube (FEDORA-2023-04473fc41e)	5435c10480	08/29/2023	08/28/2023			
284441	Fedora Security Update for youtube (FEDORA-2023-1ff11546a48)	CVE-2023-35934 FEDORA-2023-1ff11546a48	5.4	8.2	08/29/2023	08/28/2023	
284446	Fedora Security Update for xen (FEDORA-2023-04473fc41e)	CVE-2023-34320, CVE-2023-20569, CVE-2022-04473fc41e	FEDORA-2023-04473fc41e	5.4	7.5	08/29/2023	08/28/2023

1 Click Month



The screenshot shows the Qualys Cloud Platform KnowledgeBase search interface. A dropdown menu for 'Information Severity' is open, showing options like Today, Week, Month, Quarter, Year, and All. The 'Month' option is highlighted with a blue border.

Search

QID Title

QID	Title	Modified	Published
20362	IBM Db2 Privilege Escalation Vulnerability (70)	08/29/2023	08/28/2023
378800	Wireshark BT SDP dissector memory leak Vulnerability	08/29/2023	08/28/2023
378803	Wireshark CBOR dissector crash Vulnerability	08/29/2023	08/28/2023
378801	Wireshark BT SDP dissector infinite loop Vulnerability	08/29/2023	08/28/2023
691236	Free Berkeley Software Distribution (FreeBSD) (ddd3fcc9-2bdd-11ee-9af4-589fcf0f81b0)	08/29/2023	08/28/2023
378802	Wireshark CP2179 dissector crash Vulnerability	08/29/2023	08/28/2023
378810	Microsoft Edge Based on Chromium Prior to 105.0.1022.16 Vulnerabilities	08/29/2023	08/28/2023
503288	Alpine Linux Security Update for xen	08/29/2023	08/28/2023
284440	Fedora Security Update for youtube (FEDORA-2023-1ff11546a48)	08/29/2023	08/28/2023
284441	Fedora Security Update for youtube (FEDORA-2023-1ff11546a48)	08/29/2023	08/28/2023
284446	Fedora Security Update for xen (FEDORA-2023-04473fc41e)	08/29/2023	08/28/2023

1 Click the Search button

The screenshot shows the Qualys Cloud Platform interface, specifically the KnowledgeBase section. A search dialog box is open over a list of vulnerabilities.

Search Dialog Fields:

- Bugtraq ID:
- Service Modified: Select a date
- User Modified: Select a date
- Published: Previous Month
- Confirmed Severity: Level 1 Level 2 Level 3 Level 4 Level 5
- Potential Severity: Level 1 Level 2 Level 3 Level 4 Level 5
- Information Severity: Level 1 Level 2 Level 3 Level 4 Level 5
- Vendor: NOT All
- Product: NOT All
- Vulnerability Details:

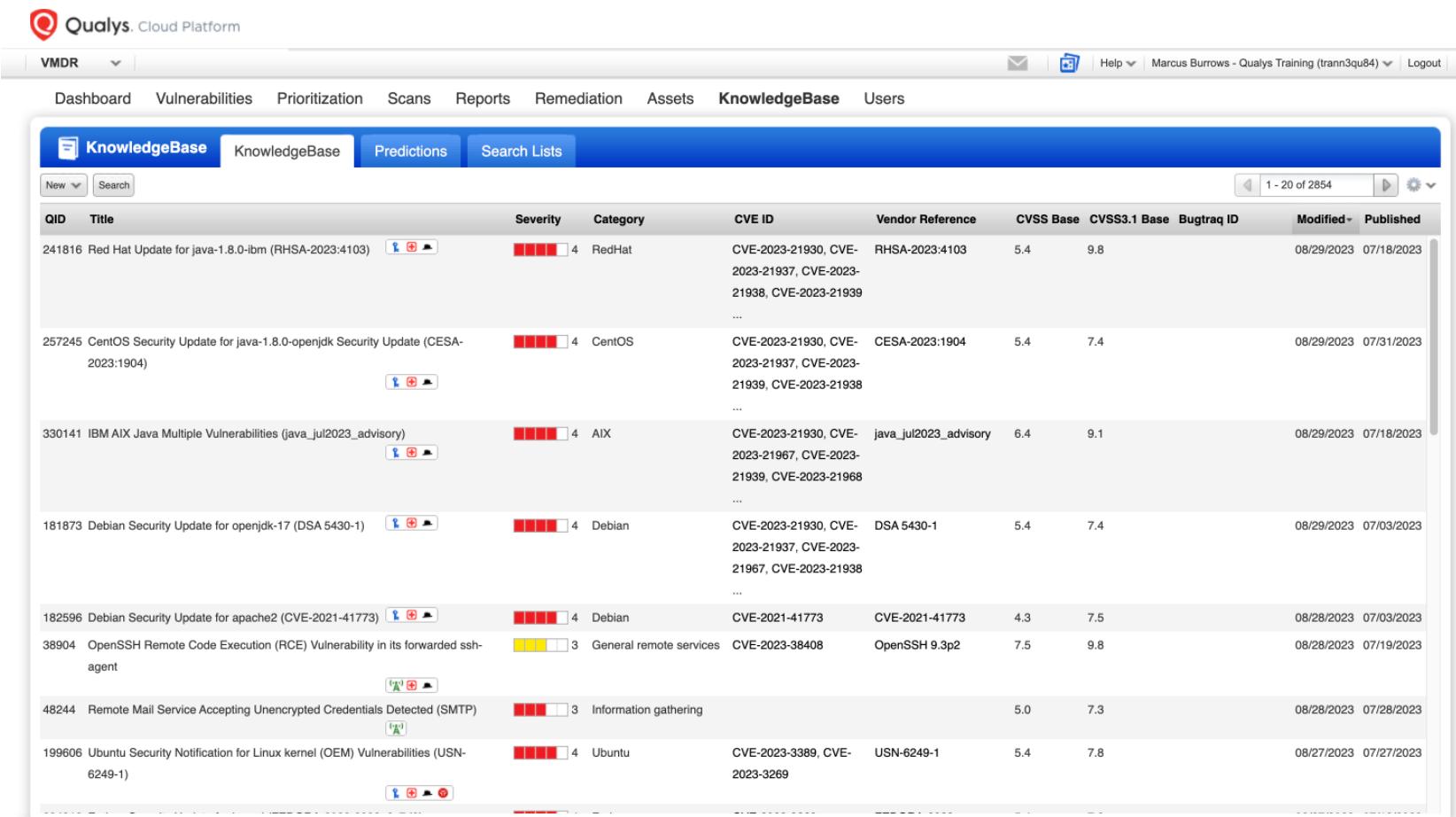
Search Button: Search

Table Headers: QID, Title, Bugtraq ID, Modified, Published

Table Data (Sample Rows):

QID	Title	Bugtraq ID	Modified	Published			
20362	IBM Db2 Privilege Escalation Vulnerability (70)		08/29/2023	08/28/2023			
378800	Wireshark BT SDP dissector memory leak Vulnerability		08/29/2023	08/28/2023			
378803	Wireshark CBOR dissector crash Vulnerability		08/29/2023	08/28/2023			
378801	Wireshark BT SDP dissector infinite loop Vulnerability		08/29/2023	08/28/2023			
691236	Free Berkeley Software Distribution (FreeBSD) (ddd3fcc9-2bdd-11ee-9af4-589fcf0f81b0)		08/29/2023	08/28/2023			
378802	Wireshark CP2179 dissector crash Vulnerability		08/29/2023	08/28/2023			
378810	Microsoft Edge Based on Chromium Prior to 103.0.1264.16 Vulnerabilities		08/29/2023	08/28/2023			
503288	Alpine Linux Security Update for xen		08/29/2023	08/28/2023			
284440	Fedora Security Update for youtube (FEDORA-2023-1ff11546a48)	5435c10480	08/29/2023	08/28/2023			
284441	Fedora Security Update for youtube (FEDORA-2023-1ff11546a48)	CVE-2023-35934	FEDORA-2023-1ff11546a48	5.4	8.2	08/29/2023	08/28/2023
284446	Fedora Security Update for xen (FEDORA-2023-04473fc41e)	CVE-2023-34320, CVE-2023-20569, CVE-2022-04473fc41e	FEDORA-2023-04473fc41e	5.4	7.5	08/29/2023	08/28/2023

- 1 Notice how the number of vulnerabilities that are displayed has been reduced. Click on the [Search](#) button again to filter the list even further.



The screenshot shows the Qualys Cloud Platform interface with the 'KnowledgeBase' tab selected. The page displays a table of vulnerabilities with the following columns: QID, Title, Severity, Category, CVE ID, Vendor Reference, CVSS Base, CVSS3.1 Base, Bugtraq ID, Modified, and Published. The table lists several entries, each with a detailed description and severity rating (e.g., 4 for RedHat, 4 for CentOS, 4 for AIX, 4 for Debian, 4 for Debian, 3 for General remote services, 3 for Information gathering, 4 for Ubuntu). The last entry is a note about Linux kernel OEM vulnerabilities. The interface includes navigation buttons for the list (1 - 20 of 2854) and a search bar at the top.

QID	Title	Severity	Category	CVE ID	Vendor Reference	CVSS Base	CVSS3.1 Base	Bugtraq ID	Modified	Published
241816	Red Hat Update for java-1.8.0-lbm (RHSA-2023:4103)		4 RedHat	CVE-2023-21930, CVE-2023-21937, CVE-2023-21938, CVE-2023-21939	RHSA-2023:4103	5.4	9.8		08/29/2023	07/18/2023
257245	CentOS Security Update for java-1.8.0-openjdk Security Update (CESA-2023:1904)		4 CentOS	CVE-2023-21930, CVE-2023-21937, CVE-2023-21939, CVE-2023-21938	CESA-2023:1904	5.4	7.4		08/29/2023	07/31/2023
330141	IBM AIX Java Multiple Vulnerabilities (java_jul2023_advisory)		4 AIX	CVE-2023-21930, CVE-2023-21967, CVE-2023-21939, CVE-2023-21968	java_jul2023_advisory	6.4	9.1		08/29/2023	07/18/2023
181873	Debian Security Update for openjdk-17 (DSA 5430-1)		4 Debian	CVE-2023-21930, CVE-2023-21937, CVE-2023-21967, CVE-2023-21938	DSA 5430-1	5.4	7.4		08/29/2023	07/03/2023
182596	Debian Security Update for apache2 (CVE-2021-41773)		4 Debian	CVE-2021-41773	CVE-2021-41773	4.3	7.5		08/28/2023	07/03/2023
38904	OpenSSH Remote Code Execution (RCE) Vulnerability in its forwarded ssh-agent		3 General remote services	CVE-2023-38408	OpenSSH 9.3p2	7.5	9.8		08/28/2023	07/19/2023
48244	Remote Mail Service Accepting Unencrypted Credentials Detected (SMTP)		3 Information gathering			5.0	7.3		08/28/2023	07/28/2023
199606	Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-6249-1)		4 Ubuntu	CVE-2023-3389, CVE-2023-3269	USN-6249-1	5.4	7.8		08/27/2023	07/27/2023

- 1 In the Search dialog box, click the scroll bar to scroll down.

The screenshot shows the Qualys Cloud Platform interface with the 'KnowledgeBase' tab selected. A search dialog box is open over the main content area. The search form includes fields for QID, Vulnerability Title, Discovery Method, Authentication Type, User Configuration, Category, Patch Solution, CVE ID, and CPE. Below the search form is a table listing various vulnerabilities with columns for ID, Title, Description, Severity, CVSS Score, and Last Modified. The table has a scroll bar on the right side, indicating it can be scrolled vertically. The search dialog also has a scroll bar on its right side, which is the focus of the task description.

- 1 Click the drop down arrow next to Vendor

The screenshot shows the Qualys Cloud Platform interface. The top navigation bar includes links for VMDR, Dashboard, Vulnerabilities, Prioritization, Scans, Reports, Remediation, Assets, KnowledgeBase (which is selected and highlighted in blue), and Users. A search bar at the top right contains the text "Marcus Burrows - Qualys Training (trann3qu84)". Below the navigation is a search panel titled "Search". The search criteria include:

- User Modified: NOT
- Published: NOT
- Confirmed Severity: Level 1 Level 2 Level 3 Level 4 Level 5
- Potential Severity: Level 1 Level 2 Level 3 Level 4 Level 5
- Information Severity: Level 1 Level 2 Level 3 Level 4 Level 5
- Vendor: NOT
- Product: NOT
- Vulnerability Details:
- Supported Modules: VM CA-Windows Agent CA-Linux Agent CA-Mac Agent
 CA-AIX Agent CA-BSD Agent CA-Solaris Agent WAS
 WAF MD GAV CSAM
 CS-Windows CS-Linux API Security SEM-IOS

A "Search" button is located at the bottom right of the search panel. To the right of the search panel, a table lists several vulnerabilities with columns for ID, Title, Published, Modified, and Bugtraq ID. The first few rows are:

ID	Title	Published	Modified	Bugtraq ID
241816	Red Hat Update for java-1.8.0-ibm (RHSA-2023:1904)	08/29/2023	07/18/2023	
257245	CentOS Security Update for java-1.8.0-openjdk-17 (DSA-2023:1904)	08/29/2023	07/31/2023	
330141	IBM AIX Java Multiple Vulnerabilities (java_ju...)	08/29/2023	07/18/2023	
181873	Debian Security Update for openjdk-17 (DSA-2023:1904)	08/29/2023	07/03/2023	
182596	Debian Security Update for apache2 (CVE-2023-38408)	08/28/2023	07/03/2023	
48244	Remote Mail Service Accepting Unencrypted...	08/28/2023	07/28/2023	
38904	OpenSSH Remote Code Execution (RCE) Vulnerability in its forwarded ssh-agent	08/28/2023	07/19/2023	
199606	Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-6249-1)	08/27/2023	07/27/2023	

Type microsoft

The screenshot shows the Qualys Cloud Platform interface, specifically the KnowledgeBase section. A search dialog is open with the term "microsoft" typed into the vendor field. The search results table lists various vulnerabilities, each with a QID, title, published date, modified date, and published date. The results include:

QID	Title	Published	Modified	Published
241816	Red Hat Update for java-1.8.0-ibm (RHSAs-2023-1904)	08/29/2023	07/18/2023	
257245	CentOS Security Update for java-1.8.0-openjdk-17 (DSA-2023-1904)	08/29/2023	07/31/2023	
330141	IBM AIX Java Multiple Vulnerabilities (java_ju...)	08/29/2023	07/18/2023	
181873	Debian Security Update for openjdk-17 (DSA-2023-1904)	08/29/2023	07/03/2023	
182596	Debian Security Update for apache2 (CVE-2023-1904)	08/28/2023	07/03/2023	
48244	Remote Mail Service Accepting Unencrypted...	08/28/2023	07/28/2023	
38904	OpenSSH Remote Code Execution (RCE) Vulnerability in its forwarded ssh-agent	08/28/2023	07/19/2023	
199606	Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-6249-1)	08/27/2023	07/27/2023	

- Click the **Search** button.

The screenshot shows the Qualys Cloud Platform interface, specifically the KnowledgeBase section. A search dialog box is open, with the vendor field set to "microsoft". The search results table lists various vulnerabilities, including:

ID	Title	Published	Modified	Published
241816	Red Hat Update for java-1.8.0-ibm (RHSAs-2023-1904)	08/29/2023	07/18/2023	
257245	CentOS Security Update for java-1.8.0-openjdk-17 (DSA-2023-1904)	08/29/2023	07/31/2023	
330141	IBM AIX Java Multiple Vulnerabilities (java_ju)	08/29/2023	07/18/2023	
181873	Debian Security Update for openjdk-17 (DSA-2023-1904)	08/29/2023	07/03/2023	
182596	Debian Security Update for apache2 (CVE-2023-3269)	08/28/2023	07/03/2023	
48244	Remote Mail Service Accepting Unencrypted	08/28/2023	07/28/2023	
38904	OpenSSH Remote Code Execution (RCE) Vulnerability in its forwarded ssh-agent	08/28/2023	07/19/2023	
199606	Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-6249-1)	08/27/2023	07/27/2023	

- 1 Notice how the total number of vulnerabilities has again been reduced. Next, click on the [Search](#) button again to filter the list even further.

The screenshot shows the Qualys Cloud Platform interface with the 'KnowledgeBase' tab selected. The main content area displays a table of vulnerabilities with the following columns: QID, Title, Severity, Category, CVE ID, Vendor Reference, CVSS Base, CVSS3.1 Base, Bugtraq ID, Modified, and Published. The table contains three rows of data:

QID	Title	Severity	Category	CVE ID	Vendor Reference	CVSS Base	CVSS3.1 Base	Bugtraq ID	Modified	Published
92033	Microsoft Windows Security Update for July 2023	4	Windows	CVE-2023-35366, CVE-2023-35309, CVE-2023-35306, CVE-2023-35305	KB5028166, KB5028168, KB5028169, KB5028171, KB5028182, KB5028185, KB5028186, KB5028222, KB5028223, KB5028224, KB5028226, KB5028228, KB5028232, KB5028233, KB5028240	10.0	9.8		08/26/2023	07/12/2023
92041	Microsoft Azure Stack Hub Security Update for July 2023	5	Windows	CVE-2023-35348, CVE-2023-35367, CVE-2023-35309, CVE-2023-35305	Azure Stack Hub	10.0	9.8		08/26/2023	07/14/2023
92037	Microsoft Windows Domain Name System (DNS) Server Remote Code Execution (RCE) Vulnerability July 2023	4	Windows	CVE-2023-35345, CVE-2023-35346, CVE-2023-35310, CVE-2023-35344	KB5028168, KB5028169, KB5028171, KB5028222, KB5028223, KB5028224, KB5028226	6.8	6.6		08/24/2023	07/12/2023

- 1 In the Search dialog box, click on the checkbox next to "No Patch Solution".

The screenshot shows the Qualys Cloud Platform interface with the 'KnowledgeBase' tab selected. A search dialog box is open, titled 'Search'. The 'Patch Solution' section contains three checkboxes: 'Patch Available', 'Trend Micro Virtual Patch Available', and 'No Patch Solution'. The 'No Patch Solution' checkbox is highlighted with a blue border, indicating it is selected. The background shows a list of vulnerabilities with columns for QID, Title, Description, Bugtraq ID, Modified, and Published dates.

QID	Title	Description	Bugtraq ID	Modified	Published
92033	Microsoft Windows Security Update for July 2023	92033 - Microsoft Windows Security Update for July 2023		08/26/2023	07/12/2023
92041	Microsoft Azure Stack Hub Security Update for July 2023	92041 - Microsoft Azure Stack Hub Security Update for July 2023		08/26/2023	07/14/2023
92037	Microsoft Windows Domain Name System (DNS) Execution (RCE) Vulnerability July 2023	92037 - Microsoft Windows Domain Name System (DNS) Execution (RCE) Vulnerability July 2023	2023-35346, CVE-2023-35347, KB5028169, KB5028222, KB5028223, KB5028224, KB5028226,	08/24/2023	07/12/2023

1 Click Search

The screenshot shows the Qualys Cloud Platform interface, specifically the KnowledgeBase section. A search dialog box is open over a list of vulnerabilities.

Search Dialog Fields:

- QID: [Input field]
- Vulnerability Title: [Input field] (with NOT checkbox)
- Discovery Method: [Dropdown: All (default)]
- Authentication Type: [Dropdown: All]
- User Configuration: [checkboxes: Disabled, Edited]
- Category: [Input field] (with NOT checkbox)
- Patch Solution: [checkboxes: Patch Available, Trend Micro Virtual Patch Available, No Patch Solution] (No Patch Solution is checked)
- CVE ID: [Input field] (with NOT checkbox) (Contains dropdown)
- CPE: [Dropdown: All]

Search Results:

QID	Title	Published	Modified
92033	Microsoft Windows Security Update for July 2023	08/26/2023	07/12/2023
92041	Microsoft Azure Stack Hub Security Update for July 2023	08/26/2023	07/14/2023
92037	Microsoft Windows Domain Name System (DNS) Execution (RCE) Vulnerability July 2023	08/24/2023	07/12/2023

Bottom Right Content:

2023-35346, CVE-2023- KB5028169 ,
35310, CVE-2023-35344 KB5028171 ,
KB5028222 ,
KB5028223 ,
KB5028224 ,
KB5028226 ,

- 1 You have filtered the list to show only Microsoft vulnerabilities that have been published within the last month, and which have no patch solution available. Click on the [drop down arrow](#) next to the first vulnerability in order to see more details.

Qualys Cloud Platform

VMDR

Dashboard Vulnerabilities Prioritization Scans Reports Remediation Assets KnowledgeBase Users

KnowledgeBase Predictions Search Lists

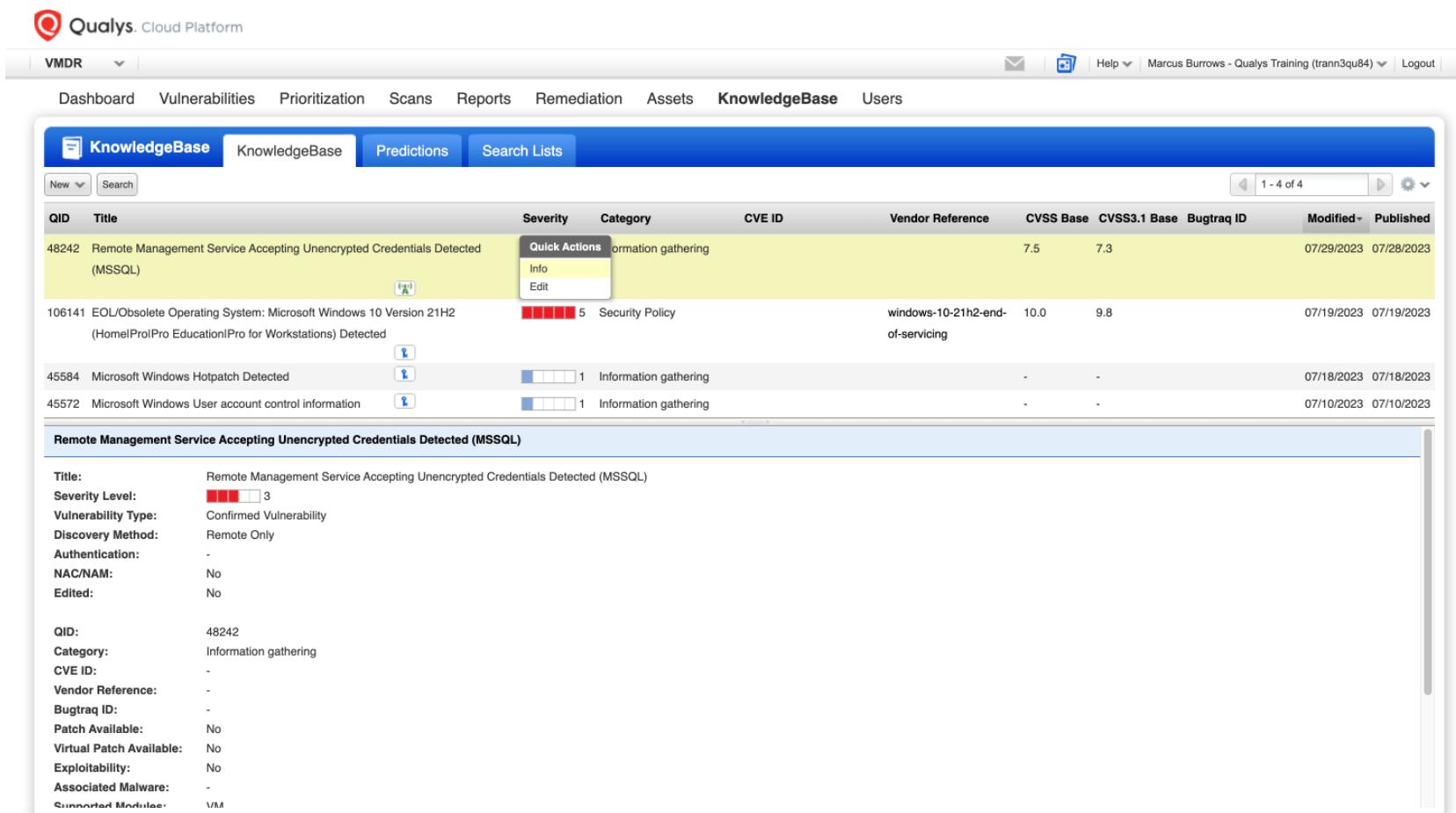
New Search

1 - 4 of 4

QID	Title	Severity	Category	CVE ID	Vendor Reference	CVSS Base	CVSS3.1 Base	Bugtraq ID	Modified	Published
48242	Remote Management Service Accepting Unencrypted Credentials Detected (MSSQL)	<div style="width: 30%;"><div style="width: 100%;">██████</div></div> 3	Information gathering			7.5	7.3		07/29/2023	07/28/2023
106141	EOL/Obsolete Operating System: Microsoft Windows 10 Version 21H2 (Home Pro Pro Education Pro for Workstations) Detected	<div style="width: 50%;"><div style="width: 100%;">██████</div></div> 5	Security Policy	windows-10-21h2-end-of-servicing	10.0	9.8		07/19/2023	07/19/2023	
45584	Microsoft Windows Hotpatch Detected	<div style="width: 10%;"><div style="width: 100%;">█</div></div> 1	Information gathering		-	-		07/18/2023	07/18/2023	
45572	Microsoft Windows User account control information	<div style="width: 10%;"><div style="width: 100%;">█</div></div> 1	Information gathering		-	-		07/10/2023	07/10/2023	

1

Click Info



The screenshot shows the Qualys Cloud Platform KnowledgeBase interface. The top navigation bar includes VMDR, Dashboard, Vulnerabilities, Prioritization, Scans, Reports, Remediation, Assets, KnowledgeBase (which is selected), and Users. A sub-navigation bar below shows KnowledgeBase, Predictions, and Search Lists. The main content area displays a table of vulnerabilities with columns for QID, Title, Severity, Category, CVE ID, Vendor Reference, CVSS Base, CVSS3.1 Base, Bugtraq ID, Modified, and Published. One row is highlighted in yellow, and a context menu is open over it with options 'Info' and 'Edit'. Below the table, a detailed view for the highlighted vulnerability is shown, titled 'Remote Management Service Accepting Unencrypted Credentials Detected (MSSQL)'. This view includes sections for General Information, Discovery, Configuration, and Associated Malware.

QID	Title	Severity	Category	CVE ID	Vendor Reference	CVSS Base	CVSS3.1 Base	Bugtraq ID	Modified	Published
48242	Remote Management Service Accepting Unencrypted Credentials Detected (MSSQL)	 3	Information gathering			7.5	7.3		07/29/2023	07/28/2023
106141	EOL/Obsolete Operating System: Microsoft Windows 10 Version 21H2 (HomePro/Pro Education/Pro for Workstations) Detected	 5	Security Policy	windows-10-21h2-end-of-servicing		10.0	9.8		07/19/2023	07/19/2023
45584	Microsoft Windows Hotpatch Detected	 1	Information gathering			-	-		07/18/2023	07/18/2023
45572	Microsoft Windows User account control information	 1	Information gathering			-	-		07/10/2023	07/10/2023

Remote Management Service Accepting Unencrypted Credentials Detected (MSSQL)

General Information

Title:	Remote Management Service Accepting Unencrypted Credentials Detected (MSSQL)
Severity Level:	 3
Vulnerability Type:	Confirmed Vulnerability
Discovery Method:	Remote Only
Authentication:	-
NAC/NAM:	No
Edited:	No

Configuration

QID:	48242
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Patch Available:	No
Virtual Patch Available:	No
Exploitability:	No
Associated Malware:	-
Supported Modules:	VM

- 1 The General Information tab shows you some important details including the Severity Level and Discovery Method. To understand these more, refer to this [article](#), then click the "**Details**" tab to continue.

Qualys Cloud Platform

VMDR

Dashboard Vulnerabilities Prioritization Scans Reports Remediation Assets KnowledgeBase Users

Vulnerability Information - QID 48242

General Information

CVSS3.1 Base	Bugtraq ID	Modified	Published
3		07/29/2023	07/28/2023
8		07/19/2023	07/19/2023
		07/18/2023	07/18/2023
		07/10/2023	07/10/2023

General Information

Details

Software

Threat

Impact

Solution

Exploitability

Associated Malware

Search Lists

Compliance

Change Log

Title: Remote Management Service Accepting Unencrypted Credentials (MSSQL)

Severity Level: 3

Vulnerability Type: Confirmed Vulnerability

Discovery Method: Remote Only

Authentication: -

NAC/NAM: No

Edited: No

Owner: -

Created: -

Service Modified: 07/29/2023 at 03:55:23 AM (GMT+0100)

User Modified: -

Published: 07/28/2023 at 01:55:01 PM (GMT+0100)

Modified By: -

Close Edit

KnowledgeBase

New Search

QID Title

48242 Remote Management Service Accepting Unencrypted Credentials (MSSQL)

106141 EOL/Obsolete Operating System: Microsoft Windows 10 (HomeProPro EducationPro for Workstations) Detected

45584 Microsoft Windows Hotpatch Detected

45572 Microsoft Windows User account control information

Remote Management Service Accepting Unencrypted Credentials

Title: Remote Management Service Accepting Unencrypted Credentials

Severity Level: 3

Vulnerability Type: Confirmed Vulnerability

Discovery Method: Remote Only

Authentication: -

NAC/NAM: No

Edited: No

QID: 48242

Category: Information gathering

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Patch Available: No

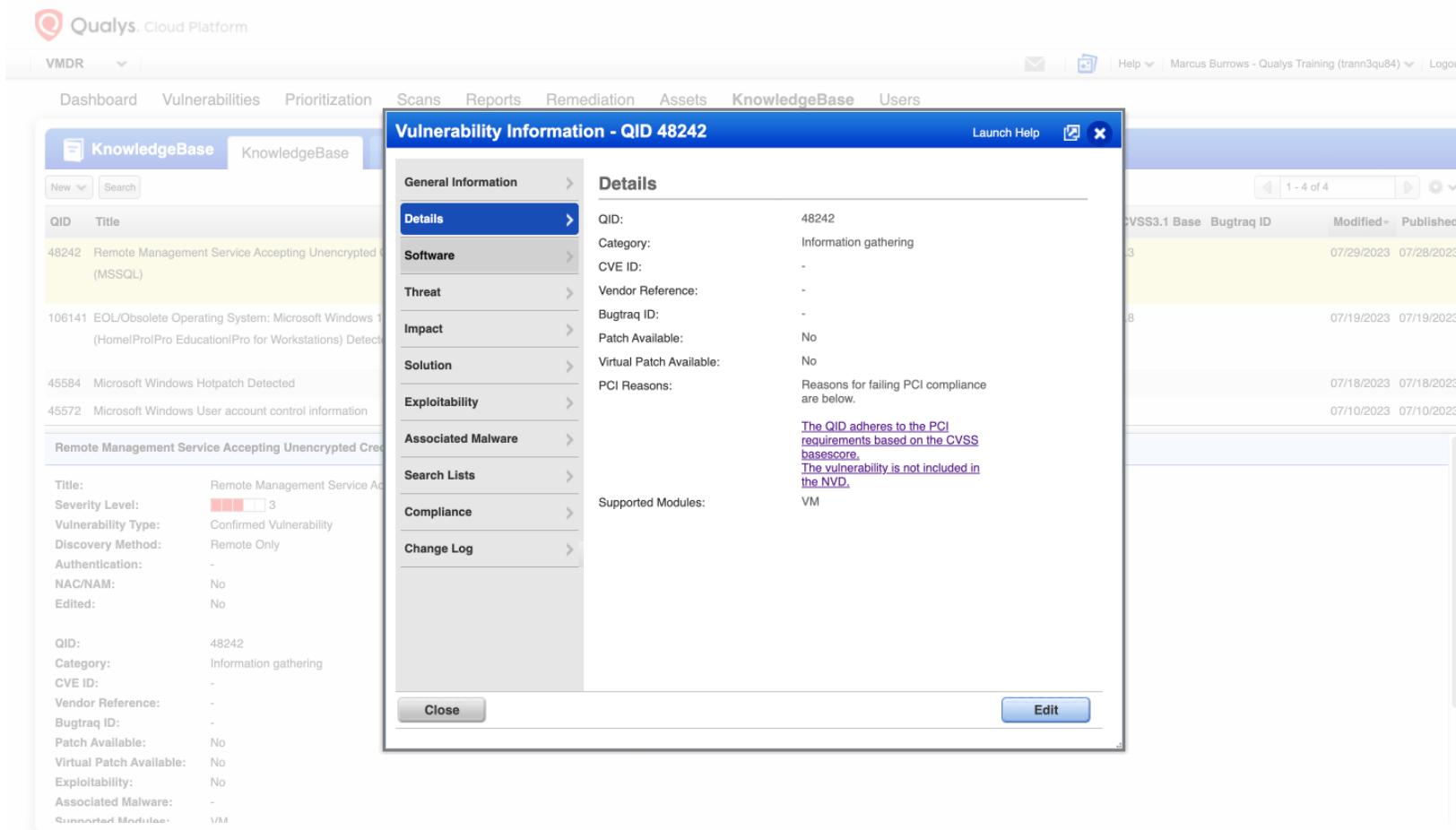
Virtual Patch Available: No

Exploitability: No

Associated Malware: -

Supported Modules: VIM

- The details tab displays CVE and vendor references, where applicable. Click on the **Software tab** to continue.



Vulnerability Information - QID 48242

General Information

- Details** (selected)
- Software**
- Threat**
- Impact**
- Solution**
- Exploitability**
- Associated Malware**
- Search Lists**
- Compliance**
- Change Log**

Details

CVSS3.1 Base	Bugtraq ID	Modified	Published
3		07/29/2023	07/28/2023
8		07/19/2023	07/19/2023
		07/18/2023	07/18/2023
		07/10/2023	07/10/2023

QID: 48242
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Patch Available: No
Virtual Patch Available: No
PCI Reasons: Reasons for failing PCI compliance are below.
[The QID adheres to the PCI requirements based on the CVSS basesscore.](#)
[The vulnerability is not included in the NVD.](#)
Supported Modules: VM

- In the Software tab, we can see the vendor and product to which this vulnerability refers. Click the Solution tab to continue.

The screenshot shows the Qualys Cloud Platform interface. The top navigation bar includes VMDR, Dashboard, Vulnerabilities, Prioritization, Scans, Reports, Remediation, Assets, KnowledgeBase (which is selected), and Users. A sidebar on the left has a KnowledgeBase tab with New and Search buttons, and a list of vulnerabilities including QID 48242, 106141, 45584, and 45572. The main content area displays 'Vulnerability Information - QID 48242'. The left sidebar under 'General Information' has sections for Details, Software (selected), Threat, Impact, Solution, Exploitability, Associated Malware, Search Lists, Compliance, and Change Log. The 'Software' section shows a table with columns 'Vendor' and 'Product'. One row shows 'microsoft' as the vendor and 'mssql-node' as the product. To the right of the main content is a table listing CVSS3.1 Base scores, Bugtraq IDs, Modified dates, and Published dates for various entries. The table has columns for CVSS3.1 Base, Bugtraq ID, Modified, and Published. Rows include:

CVSS3.1 Base	Bugtraq ID	Modified	Published
3		07/29/2023	07/28/2023
8		07/19/2023	07/19/2023
		07/18/2023	07/18/2023
		07/10/2023	07/10/2023

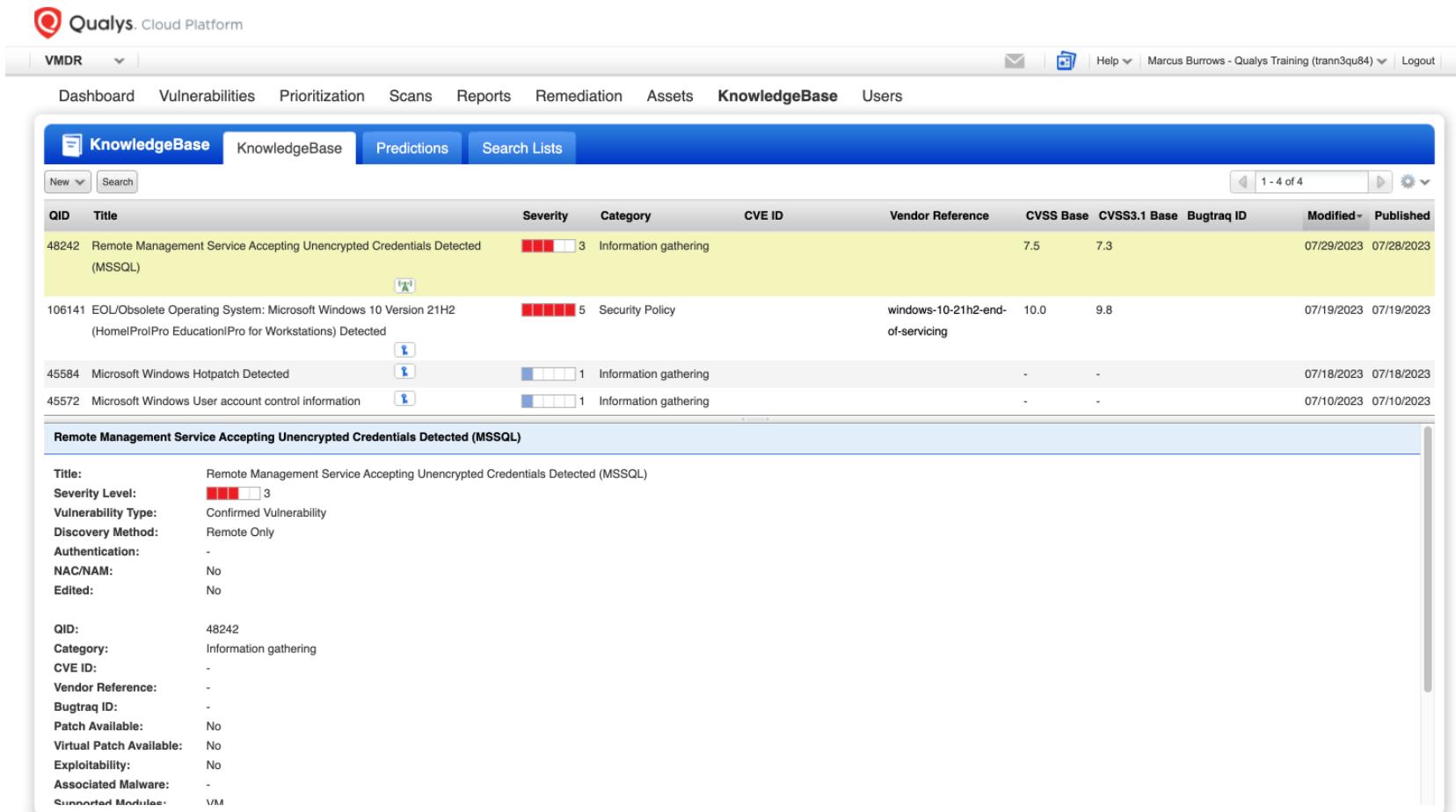
- 1 Sometimes the Solution tab will display patch details. There is no relevant patch for this vulnerability, but a recommended action is given instead. Click the [Close](#) button.

The screenshot shows the Qualys Cloud Platform interface. The top navigation bar includes VMDR, Dashboard, Vulnerabilities, Prioritization, Scans, Reports, Remediation, Assets, KnowledgeBase (which is selected), and Users. A sidebar on the left has a KnowledgeBase section with New, Search, QID, and Title filters. Below this are lists of vulnerabilities: QID 48242 (Remote Management Service Accepting Unencrypted (MSSQL)), QID 106141 (EOL/Obsolete Operating System: Microsoft Windows 10 (HomePro/Pro Education/Pro for Workstations) Detected), QID 45584 (Microsoft Windows Hotpatch Detected), and QID 45572 (Microsoft Windows User account control information). The main content area displays a 'Vulnerability Information - QID 48242' dialog. The 'Solution' tab is active, containing the following text: 'If possible, use alternate services that provide encryption. Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission.' Below the dialog is a table of CVSS3.1 scores and dates:

CVSS3.1 Base	Bugtraq ID	Modified	Published
3		07/29/2023	07/28/2023
8		07/19/2023	07/19/2023
		07/18/2023	07/18/2023
		07/10/2023	07/10/2023

At the bottom of the dialog are 'Close' and 'Edit' buttons.

1 Click the second vulnerability in the list to continue.



The screenshot shows the Qualys Cloud Platform KnowledgeBase interface. The top navigation bar includes VMDR, Dashboard, Vulnerabilities, Prioritization, Scans, Reports, Remediation, Assets, KnowledgeBase (which is selected), and Users. The KnowledgeBase tab has sub-options: New, Search, Predictions, and Search Lists. The main table displays vulnerabilities with columns: QID, Title, Severity, Category, CVE ID, Vendor Reference, CVSS Base, CVSS3.1 Base, Bugtraq ID, Modified, and Published. The second row, titled "EOL/Obsolete Operating System: Microsoft Windows 10 Version 21H2 (HomePro/Pro Education/Pro for Workstations) Detected", is highlighted with a yellow background and a blue border. A modal window for this specific vulnerability is open, showing detailed information including Title, Severity Level (3), Vulnerability Type (Confirmed Vulnerability), Discovery Method (Remote Only), Authentication (-), NAC/NAM (No), Edited (No), QID (48242), Category (Information gathering), CVE ID (-), Vendor Reference (-), Bugtraq ID (-), Patch Available (No), Virtual Patch Available (No), Exploitability (No), Associated Malware (-), and Supported Modules (VM).

QID	Title	Severity	Category	CVE ID	Vendor Reference	CVSS Base	CVSS3.1 Base	Bugtraq ID	Modified	Published
48242	Remote Management Service Accepting Unencrypted Credentials Detected (MSSQL)	<div style="width: 30px; height: 10px; background-color: red;"></div> <div style="width: 20px; height: 10px; background-color: white;"></div>	3	Information gathering		7.5	7.3		07/29/2023	07/28/2023
106141	EOL/Obsolete Operating System: Microsoft Windows 10 Version 21H2 (HomePro/Pro Education/Pro for Workstations) Detected	<div style="width: 50px; height: 10px; background-color: red;"></div> <div style="width: 10px; height: 10px; background-color: white;"></div>	5	Security Policy	windows-10-21h2-end-of-servicing	10.0	9.8		07/19/2023	07/19/2023
45584	Microsoft Windows Hotpatch Detected	<div style="width: 10px; height: 10px; background-color: blue;"></div> <div style="width: 10px; height: 10px; background-color: white;"></div>	1	Information gathering		-	-		07/18/2023	07/18/2023
45572	Microsoft Windows User account control information	<div style="width: 10px; height: 10px; background-color: blue;"></div> <div style="width: 10px; height: 10px; background-color: white;"></div>	1	Information gathering		-	-		07/10/2023	07/10/2023

Remote Management Service Accepting Unencrypted Credentials Detected (MSSQL)

Title: Remote Management Service Accepting Unencrypted Credentials Detected (MSSQL)
Severity Level: 3
Vulnerability Type: Confirmed Vulnerability
Discovery Method: Remote Only
Authentication: -
NAC/NAM: No
Edited: No

QID: 48242
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Patch Available: No
Virtual Patch Available: No
Exploitability: No
Associated Malware: -
Supported Modules: VM

- 1 Click the drop down arrow next to the second vulnerability.

The screenshot shows the Qualys Cloud Platform KnowledgeBase interface. The top navigation bar includes VMDR, Dashboard, Vulnerabilities, Prioritization, Scans, Reports, Remediation, Assets, KnowledgeBase (which is selected), and Users. The main content area has tabs for KnowledgeBase, Predictions, and Search Lists. A search bar and a page number indicator (1 - 4 of 4) are also present. The table lists vulnerabilities with columns for QID, Title, Severity, Category, CVE ID, Vendor Reference, CVSS Base, CVSS3.1 Base, Bugtraq ID, Modified, and Published. The second row, titled "EOL/Obsolete Operating System: Microsoft Windows 10 Version 21H2 (HomePro/Pro Education/Pro for Workstations) Detected", has a dropdown arrow icon next to its title. A detailed view of this specific vulnerability is shown in a modal window at the bottom left, containing fields like Title, Severity Level, Vulnerability Type, Discovery Method, Authentication, NAC/NAM, Edited, QID, Category, CVE ID, Vendor Reference, Bugtraq ID, Patch Available, Virtual Patch Available, Exploitability, Associated Malware, and Supported Modules.

QID	Title	Severity	Category	CVE ID	Vendor Reference	CVSS Base	CVSS3.1 Base	Bugtraq ID	Modified	Published
48242	Remote Management Service Accepting Unencrypted Credentials Detected (MSSQL)	<div style="width: 30px; height: 10px; background-color: red;"></div>	Information gathering			7.5	7.3		07/29/2023	07/28/2023
106141	EOL/Obsolete Operating System: Microsoft Windows 10 Version 21H2 (HomePro/Pro Education/Pro for Workstations) Detected	<div style="width: 50px; height: 10px; background-color: red;"></div>	Security Policy	windows-10-21h2-end-of-servicing	10.0	9.8			07/19/2023	07/19/2023
45584	Microsoft Windows Hotpatch Detected	<div style="width: 10px; height: 10px; background-color: blue;"></div>	Information gathering		-	-			07/18/2023	07/18/2023
45572	Microsoft Windows User account control information	<div style="width: 10px; height: 10px; background-color: blue;"></div>	Information gathering		-	-			07/10/2023	07/10/2023

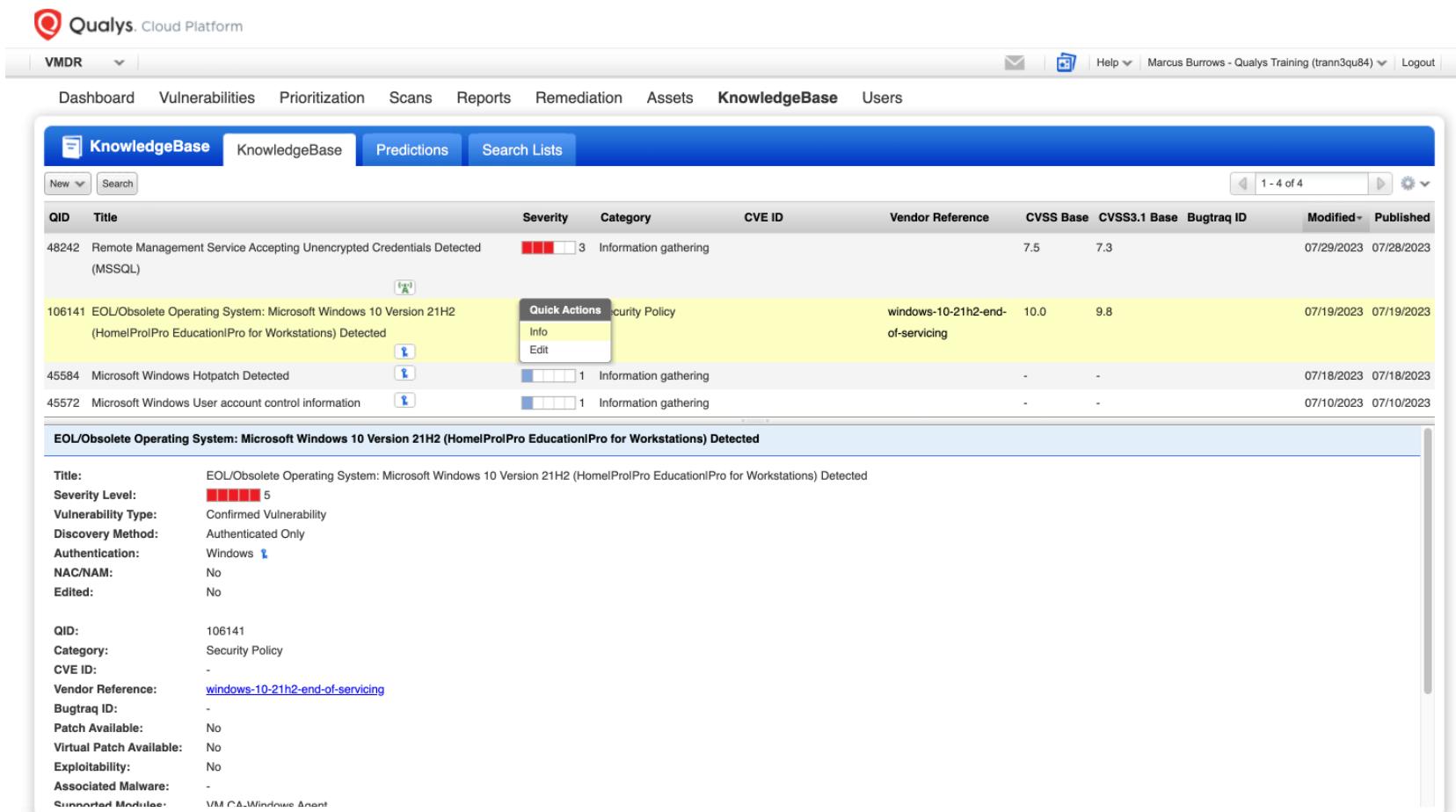
Remote Management Service Accepting Unencrypted Credentials Detected (MSSQL)

Title: Remote Management Service Accepting Unencrypted Credentials Detected (MSSQL)
Severity Level: 3
Vulnerability Type: Confirmed Vulnerability
Discovery Method: Remote Only
Authentication: -
NAC/NAM: No
Edited: No

QID: 48242
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Patch Available: No
Virtual Patch Available: No
Exploitability: No
Associated Malware: -
Supported Modules: VIM

1

Click Info



The screenshot shows the Qualys Cloud Platform KnowledgeBase interface. The top navigation bar includes VMDR, Dashboard, Vulnerabilities, Prioritization, Scans, Reports, Remediation, Assets, KnowledgeBase (which is selected), and Users. The main content area has tabs for KnowledgeBase, Predictions, and Search Lists. A search bar and a navigation bar with '1 - 4 of 4' are visible. The main table lists vulnerabilities with columns for QID, Title, Severity, Category, CVE ID, Vendor Reference, CVSS Base, CVSS3.1 Base, Bugtraq ID, Modified, and Published. One row is highlighted in yellow, and a context menu 'Quick Actions' is open over it, showing 'Info' (which is selected) and 'Edit'. Below this table is a detailed view for vulnerability QID 106141, titled 'EOL/Obsolete Operating System: Microsoft Windows 10 Version 21H2 (Home|Pro|Education|Pro for Workstations) Detected'. The detailed view includes sections for General Information, Configuration, and Associated Malware.

QID	Title	Severity	Category	CVE ID	Vendor Reference	CVSS Base	CVSS3.1 Base	Bugtraq ID	Modified	Published
48242	Remote Management Service Accepting Unencrypted Credentials Detected (MSSQL)	<div style="width: 30px; height: 10px; background-color: red;"></div> <div style="width: 70px; height: 10px; background-color: yellow;"></div>	3	Information gathering		7.5	7.3		07/29/2023	07/28/2023
106141	EOL/Obsolete Operating System: Microsoft Windows 10 Version 21H2 (Home Pro Education Pro for Workstations) Detected	<div style="width: 50px; height: 10px; background-color: red;"></div> <div style="width: 50px; height: 10px; background-color: yellow;"></div>	5	Security Policy	windows-10-21h2-end-of-servicing	10.0	9.8		07/19/2023	07/19/2023
45584	Microsoft Windows Hotpatch Detected	<div style="width: 10px; height: 10px; background-color: blue;"></div> <div style="width: 90px; height: 10px; background-color: yellow;"></div>	1	Information gathering		-	-		07/18/2023	07/18/2023
45572	Microsoft Windows User account control information	<div style="width: 10px; height: 10px; background-color: blue;"></div> <div style="width: 90px; height: 10px; background-color: yellow;"></div>	1	Information gathering		-	-		07/10/2023	07/10/2023

EOL/Obsolete Operating System: Microsoft Windows 10 Version 21H2 (Home|Pro|Education|Pro for Workstations) Detected

General Information

Title:	EOL/Obsolete Operating System: Microsoft Windows 10 Version 21H2 (Home Pro Education Pro for Workstations) Detected
Severity Level:	<div style="width: 50px; height: 10px; background-color: red;"></div> <div style="width: 50px; height: 10px; background-color: yellow;"></div> 5

- 1 Why do you think the Severity Level is 5 (Urgent) for this vulnerability? Refer to this [article](#) for more information. What is the generic description for the "Urgent" Severity Level? Click the [Software tab](#) to continue.

Qualys Cloud Platform

VMDR

Dashboard Vulnerabilities Prioritization Scans Reports Remediation Assets KnowledgeBase Users

Vulnerability Information - QID 106141

General Information

CVSS3.1 Base	Bugtraq ID	Modified	Published
3		07/29/2023	07/28/2023
8		07/19/2023	07/19/2023
		07/18/2023	07/18/2023
		07/10/2023	07/10/2023

General Information

Title: EOL/Obsolete Operating System: Microsoft Windows 10 Version 21H2 (Home|Pro|Education|Pro for Workstations) Detected

Severity Level: 5

Vulnerability Type: Confirmed Vulnerability

Discovery Method: Authenticated Only

Authentication: Windows

NAC/NAM: No

Edited: No

Owner: -

Created: -

Service Modified: 07/19/2023 at 07:07:27 PM (GMT+0100)

User Modified: -

Published: 07/19/2023 at 04:27:03 PM (GMT+0100)

Modified By: -

Details

Software

Threat

Impact

Solution

Exploitability

Associated Malware

Search Lists

Compliance

Change Log

Close Edit

QID: 106141

Category: Security Policy

CVE ID: -

Vendor Reference: [windows-10-21h2-end-of-service](#)

Bugtraq ID: -

Patch Available: No

Virtual Patch Available: No

Exploitability: No

Associated Malware: -

Supported Modules: VMCA Windows Agent

- 1 We can see again the vendor and product to which this vulnerability refers. Click on the Threat tab to continue.

The screenshot shows the Qualys Cloud Platform interface. The main navigation bar includes VMDR, Dashboard, Vulnerabilities, Prioritization, Scans, Reports, Remediation, Assets, KnowledgeBase, and Users. A sub-menu under KnowledgeBase shows 'New' and 'Search' options. The central window displays 'Vulnerability Information - QID 106141'. The left sidebar lists several vulnerabilities, including QID 48242, 106141, 45584, and 45572. The main content area shows 'General Information' with sections for Details, Software, Threat, Impact, Solution, Exploitability, Associated Malware, Search Lists, Compliance, and Change Log. Under 'Software', it lists 'Vendor' as microsoft and 'Product' as windows. Below this is a table with columns for CVSS3.1 Base, Bugtraq ID, Modified, and Published. The table contains four rows with data: (3, 07/29/2023, 07/28/2023), (8, 07/19/2023, 07/19/2023), (8, 07/18/2023, 07/18/2023), and (8, 07/10/2023, 07/10/2023). At the bottom of the central window are 'Close' and 'Edit' buttons.

- 1 The Threat tab provides more details as to the nature of the threat and the specific editions of Windows which are affected. This could then be used to help guide our remediation strategy. Click on the [Impact tab](#) to continue.

Qualys Cloud Platform

VMDR

Dashboard Vulnerabilities Prioritization Scans Reports Remediation Assets KnowledgeBase Users

Vulnerability Information - QID 106141

General Information

Details

Software

Threat

Impact

Solution

Exploitability

Associated Malware

Search Lists

Compliance

Change Log

Threat

Windows 10, version 21H2 will reach end of servicing on June 13, 2023.

This applies to the following editions released in November of 2021:

Windows 10 Home, version 21H2
Windows 10 Pro, version 21H2
Windows 10 Pro Education, version 21H2
Windows 10 Pro for Workstations, version 21H2

Microsoft no longer releases security patches and encourages customers to update to a supported version of Windows 10 Version 21H2.

CVSS3.1 Base Bugtraq ID Modified Published

CVSS3.1 Base	Bugtraq ID	Modified	Published
3		07/29/2023	07/28/2023
8		07/19/2023	07/19/2023
		07/18/2023	07/18/2023
		07/10/2023	07/10/2023

Close Edit

QID Title

48242 Remote Management Service Accepting Unencrypted (MSSQL)

106141 EOL/Obsolete Operating System: Microsoft Windows 10 Version 21H2 (Home|Pro|Pro Education|Pro for Workstations) Detected

45584 Microsoft Windows Hotpatch Detected

45572 Microsoft Windows User account control information

EOL/Obsolete Operating System: Microsoft Windows 10 Version 21H2

Title: EOL/Obsolete Operating System

Severity Level: 5

Vulnerability Type: Confirmed Vulnerability

Discovery Method: Authenticated Only

Authentication: Windows

NAC/NAM: No

Edited: No

QID: 106141

Category: Security Policy

CVE ID: -

Vendor Reference: [windows-10-21h2-end-of-service](#)

Bugtraq ID: -

Patch Available: No

Virtual Patch Available: No

Exploitability: No

Associated Malware: -

Supported Modules: VMCA Windows Agent

i The Impact tab explains why the Severity Level is the highest. Click on the **Close** button to continue.

Qualys Cloud Platform

VMDR

Dashboard Vulnerabilities Prioritization Scans Reports Remediation Assets KnowledgeBase Users

Vulnerability Information - QID 106141

General Information >

Details >

Software >

Threat >

Impact > (Selected)

Solution >

Exploitability >

Associated Malware >

Search Lists >

Compliance >

Change Log >

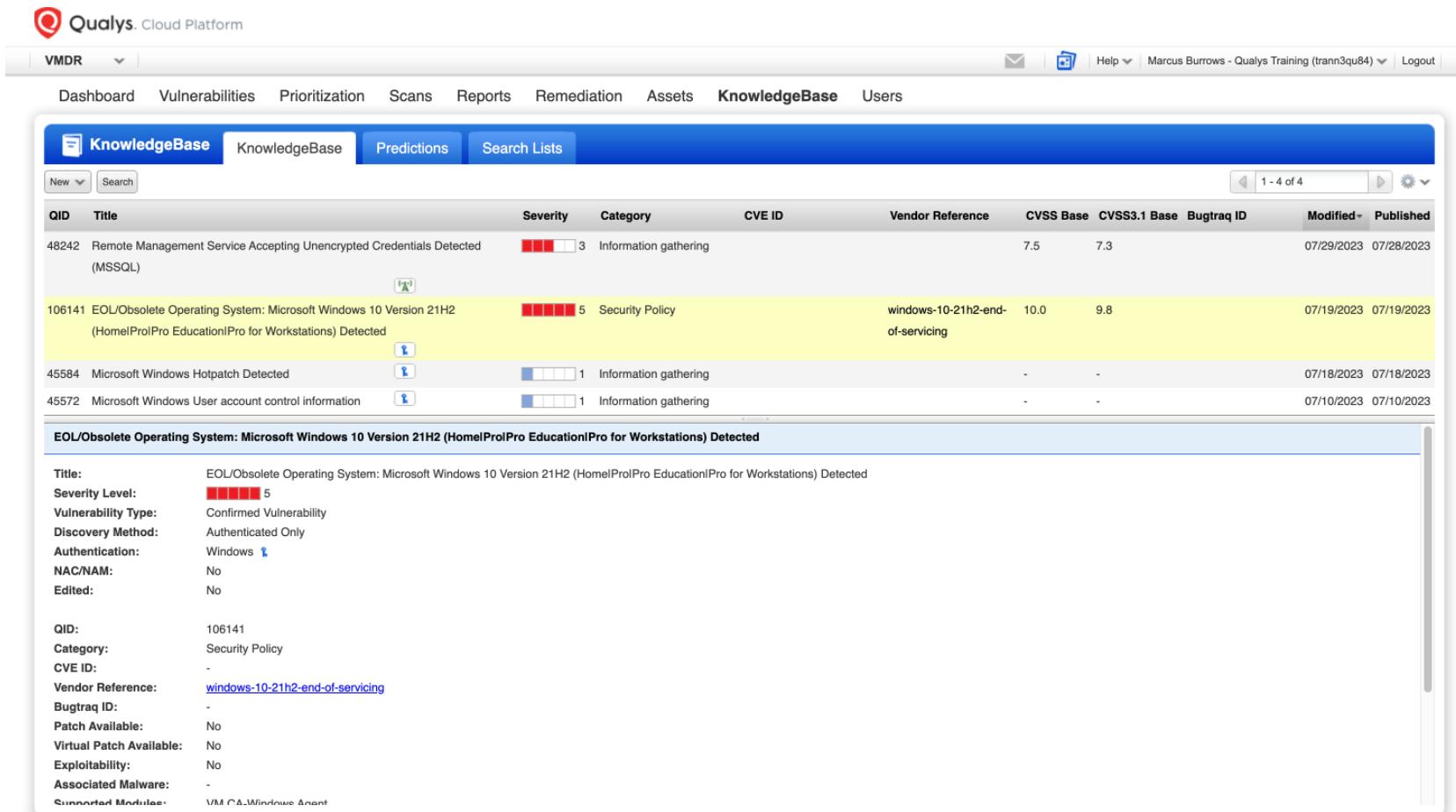
Impact

Microsoft no longer provides security updates. Obsolete software is more vulnerable to viruses and other attacks.

Close **Edit**

CVSS3.1 Base	Bugtraq ID	Modified	Published
1.3		07/29/2023	07/28/2023
1.8		07/19/2023	07/19/2023
		07/18/2023	07/18/2023
		07/10/2023	07/10/2023

1 Now click on the **last vulnerability** in the list.



The screenshot shows the Qualys Cloud Platform KnowledgeBase interface. The navigation bar includes VMDR, Dashboard, Vulnerabilities, Prioritization, Scans, Reports, Remediation, Assets, KnowledgeBase (selected), and Users. The KnowledgeBase tab is active, displaying a table of vulnerabilities. The table columns are: QID, Title, Severity, Category, CVE ID, Vendor Reference, CVSS Base, CVSS3.1 Base, Bugtraq ID, Modified, and Published. The last row, QID 106141, is highlighted with a yellow background. This row details a vulnerability titled "EOL/Obsolete Operating System: Microsoft Windows 10 Version 21H2 (Home|Pro|Education|Pro for Workstations) Detected". The detailed view in the modal dialog provides specific information for this vulnerability, including its title, severity level (5), category (Security Policy), vendor reference (windows-10-21h2-end-of-servicing), and various CVSS metrics.

QID	Title	Severity	Category	CVE ID	Vendor Reference	CVSS Base	CVSS3.1 Base	Bugtraq ID	Modified	Published
48242	Remote Management Service Accepting Unencrypted Credentials Detected (MSSQL)	<div style="width: 30px; height: 10px; background-color: red;"></div> <div style="width: 70px; height: 10px; background-color: white;"></div>	3	Information gathering		7.5	7.3		07/29/2023	07/28/2023
106141	EOL/Obsolete Operating System: Microsoft Windows 10 Version 21H2 (Home Pro Education Pro for Workstations) Detected	<div style="width: 100px; height: 10px; background-color: red;"></div> <div style="width: 10px; height: 10px; background-color: white;"></div>	5	Security Policy	windows-10-21h2-end-of-servicing	10.0	9.8		07/19/2023	07/19/2023
45584	Microsoft Windows Hotpatch Detected	<div style="width: 10px; height: 10px; background-color: blue;"></div> <div style="width: 90px; height: 10px; background-color: white;"></div>	1	Information gathering		-	-		07/18/2023	07/18/2023
45572	Microsoft Windows User account control information	<div style="width: 10px; height: 10px; background-color: blue;"></div> <div style="width: 90px; height: 10px; background-color: white;"></div>	1	Information gathering		-	-		07/10/2023	07/10/2023

EOL/Obsolete Operating System: Microsoft Windows 10 Version 21H2 (Home|Pro|Education|Pro for Workstations) Detected

Title: EOL/Obsolete Operating System: Microsoft Windows 10 Version 21H2 (Home|Pro|Education|Pro for Workstations) Detected
Severity Level: 5
Vulnerability Type: Confirmed Vulnerability
Discovery Method: Authenticated Only
Authentication: Windows 
NAC/NAM: No
Edited: No

QID: 106141
Category: Security Policy
CVE ID: -
Vendor Reference: [windows-10-21h2-end-of-servicing](#)
Bugtraq ID: -
Patch Available: No
Virtual Patch Available: No
Exploitability: No
Associated Malware: -
Supported Modules: VM GAD Windows Agent

1 Click the drop down arrow.

The screenshot shows the Qualys Cloud Platform interface. The top navigation bar includes 'VMDR' (selected), 'Dashboard', 'Vulnerabilities', 'Prioritization', 'Scans', 'Reports', 'Remediation', 'Assets', 'KnowledgeBase' (selected), and 'Users'. A dropdown menu is open over the 'KnowledgeBase' tab, with the 'Search Lists' option highlighted. The main content area displays a table of vulnerabilities:

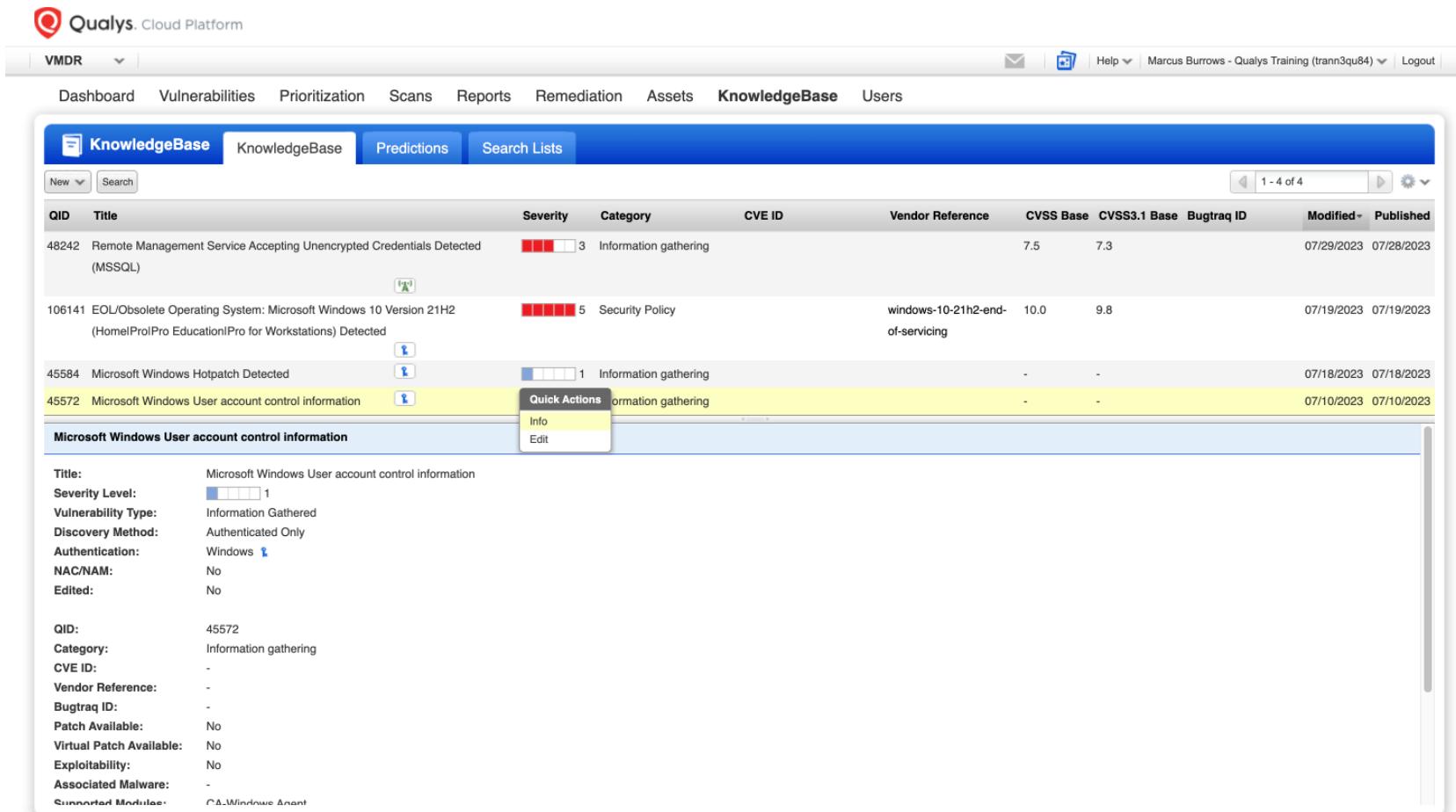
QID	Title	Severity	Category	CVE ID	Vendor Reference	CVSS Base	CVSS3.1 Base	Bugtraq ID	Modified	Published
48242	Remote Management Service Accepting Unencrypted Credentials Detected (MSSQL)	<div style="width: 30px; height: 10px; background-color: red;"></div>	3	Information gathering		7.5	7.3		07/29/2023	07/28/2023
106141	EOL/Obsolete Operating System: Microsoft Windows 10 Version 21H2 (Home Pro Education Pro for Workstations) Detected	<div style="width: 50px; height: 10px; background-color: red;"></div>	5	Security Policy	windows-10-21h2-end-of-servicing	10.0	9.8		07/19/2023	07/19/2023
45584	Microsoft Windows Hotpatch Detected	<div style="width: 10px; height: 10px; background-color: blue;"></div>	1	Information gathering		-	-		07/18/2023	07/18/2023
45572	Microsoft Windows User account control information	<div style="width: 10px; height: 10px; background-color: blue;"></div>	1	Information gathering		-	-		07/10/2023	07/10/2023

A detailed view of the second vulnerability (QID 106141) is shown in a modal window:

EOL/Obsolete Operating System: Microsoft Windows 10 Version 21H2 (Home|Pro|Education|Pro for Workstations) Detected

Title:	EOL/Obsolete Operating System: Microsoft Windows 10 Version 21H2 (Home Pro Education Pro for Workstations) Detected
Severity Level:	<div style="width: 50px; height: 10px; background-color: red;"></div> 5
Vulnerability Type:	Confirmed Vulnerability
Discovery Method:	Authenticated Only
Authentication:	Windows
NAC/NAM:	No
Edited:	No
QID:	106141
Category:	Security Policy
CVE ID:	-
Vendor Reference:	windows-10-21h2-end-of-servicing
Bugtraq ID:	-
Patch Available:	No
Virtual Patch Available:	No
Exploitability:	No
Associated Malware:	-
Supported Modules:	VM G&A Windows Agent

1 Click Info



The screenshot shows the Qualys Cloud Platform interface with the 'KnowledgeBase' tab selected. A list of vulnerabilities is displayed, including:

QID	Title	Severity	Category	CVE ID	Vendor Reference	CVSS Base	CVSS3.1 Base	Bugtraq ID	Modified	Published
48242	Remote Management Service Accepting Unencrypted Credentials Detected (MSSQL)	3	Information gathering			7.5	7.3		07/29/2023	07/28/2023
106141	EOL/Obsolete Operating System: Microsoft Windows 10 Version 21H2 (HomePro/Pro Education/Pro for Workstations) Detected	5	Security Policy	windows-10-21h2-end-of-servicing	10.0	9.8			07/19/2023	07/19/2023
45584	Microsoft Windows Hotpatch Detected	1	Information gathering			-	-		07/18/2023	07/18/2023
45572	Microsoft Windows User account control information	1	Information gathering			-	-		07/10/2023	07/10/2023

A specific row for 'Microsoft Windows User account control information' (QID: 45572) is highlighted in yellow. A context menu is open over this row, with 'Info' being the selected option. The detailed view for this vulnerability shows:

Title:	Microsoft Windows User account control information
Severity Level:	1
Vulnerability Type:	Information Gathered
Discovery Method:	Authenticated Only
Authentication:	Windows
NAC/NAM:	No
Edited:	No
QID:	45572
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Patch Available:	No
Virtual Patch Available:	No
Exploitability:	No
Associated Malware:	-
Supported Modules:	Δ Windows Agent

- 1 We can see that this Q.I.D. is not a vulnerability as such, but "Information Gathered". When included in the results of a scan, it will show user account control information. Click [Details](#) to continue.

The screenshot shows the Qualys Cloud Platform interface. The top navigation bar includes VMDR, Dashboard, Vulnerabilities, Prioritization, Scans, Reports, Remediation, Assets, KnowledgeBase, and Users. A message bar at the top right indicates "Marcus Burrows - Qualys Training (trann3qu84) Logout". The main content area displays the "Vulnerability Information - QID 45572" dialog box. The dialog has a "General Information" tab selected, showing details such as Title (Microsoft Windows User account control information), Severity Level (1), Vulnerability Type (Information Gathered), and Discovery Method (Authenticated Only). Other tabs include Software, Threat, Impact, Solution, Exploitability, Associated Malware, Search Lists, Compliance, and Change Log. Below the dialog is a table listing vulnerabilities with columns for CVSS3.1 Base, Bugtraq ID, Modified, and Published. The table shows four entries, with the fourth entry highlighted in yellow.

CVSS3.1 Base	Bugtraq ID	Modified	Published
3		07/29/2023	07/28/2023
8		07/19/2023	07/19/2023
8		07/18/2023	07/18/2023
		07/10/2023	07/10/2023

- 1 The Details tab, not surprisingly, does not show CVE or vendor references, as this is an Information Gathered Q.I.D. and not a discovered vulnerability. Click on the [Software tab](#) to continue.

The screenshot shows the Qualys Cloud Platform interface. On the left, there's a sidebar with 'KnowledgeBase' selected. The main area displays a 'Vulnerability Information - QID 45572' dialog. The 'Details' tab is active, showing the following information:

Category	Value
QID:	45572
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Patch Available:	No
Virtual Patch Available:	No
Supported Modules:	CA-Windows Agent

Below the details, there are tabs for Software, Threat, Impact, Solution, Exploitability, Associated Malware, Search Lists, Compliance, and Change Log. At the bottom of the dialog are 'Close' and 'Edit' buttons. To the right of the dialog, there's a list of vulnerabilities with columns for CVSS3.1 Base, Bugtraq ID, Modified, and Published. The first item in the list is:

CVSS3.1 Base	Bugtraq ID	Modified	Published
3		07/29/2023	07/28/2023

1 As before, the Software tab shows us the vendor and product. Click on the Threat tab to continue.

The screenshot shows the Qualys Cloud Platform interface. The main title is "Vulnerability Information - QID 45572". On the left, there's a sidebar with a "KnowledgeBase" section containing a table with rows for QID, Title, and Description. Below this are sections for Microsoft Windows User account control information, QID details, and supported modules. The main content area has a "Software" tab selected, showing a table with columns "Vendor" and "Product". The vendor is listed as "microsoft" and the product as "windows". To the right, there's a large panel displaying a list of vulnerabilities with columns for CVSS3.1 Base, Bugtraq ID, Modified, and Published. There are four items listed, each with a timestamp of 07/28/2023 or 07/19/2023.

CVSS3.1 Base	Bugtraq ID	Modified	Published
3		07/29/2023	07/28/2023
8		07/19/2023	07/19/2023
		07/18/2023	07/18/2023
		07/10/2023	07/10/2023

- 1 The Threat tab explains what this Q.I.D. is about, which in this case means describing what information the Q.I.D. reveals. Click the **Close button** to continue.

The screenshot shows the Qualys Cloud Platform interface. On the left, there's a sidebar with 'KnowledgeBase' selected. The main area displays a 'Vulnerability Information - QID 45572' window. This window has a sidebar with tabs: General Information, Details, Software, Threat (which is selected), Impact, Solution, Exploitability, Associated Malware, Search Lists, Compliance, and Change Log. The 'Threat' tab contains the following text:
This QID lists Windows User Account Control (UAC) information on the Windows system.
The account information found is listed in the Results section.
Below this, there's a table with four rows, each containing CVSS3.1 Base, Bugtraq ID, Modified, and Published columns. The first row is highlighted in yellow. The table data is as follows:

CVSS3.1 Base	Bugtraq ID	Modified	Published
3		07/29/2023	07/28/2023
8		07/19/2023	07/19/2023
07/18/2023	07/18/2023	07/10/2023	07/10/2023

At the bottom of the 'Threat' window are 'Close' and 'Edit' buttons. The overall interface is clean with a light blue header and a white body.

- 1 In this lab you have learned how to filter the KnowledgeBase and learned more about the details included for each vulnerability entry. That's it, you're done. You may now close this browser tab.

The screenshot shows the Qualys Cloud Platform interface with the 'KnowledgeBase' tab selected. The main area displays a table of vulnerabilities:

QID	Title	Severity	Category	CVE ID	Vendor Reference	CVSS Base	CVSS3.1 Base	Bugtraq ID	Modified	Published
48242	Remote Management Service Accepting Unencrypted Credentials Detected (MSSQL)	3	Information gathering			7.5	7.3		07/29/2023	07/28/2023
106141	EOL/Obsolete Operating System: Microsoft Windows 10 Version 21H2 (Home Pro Education Pro for Workstations) Detected	5	Security Policy		windows-10-21h2-end-of-servicing	10.0	9.8		07/19/2023	07/19/2023
45584	Microsoft Windows Hotpatch Detected	1	Information gathering			-	-		07/18/2023	07/18/2023
45572	Microsoft Windows User account control information	1	Information gathering			-	-		07/10/2023	07/10/2023

A detailed view of the last row (QID 45572) is expanded:

Microsoft Windows User account control information	
Title:	Microsoft Windows User account control information
Severity Level:	1
Vulnerability Type:	Information Gathered
Discovery Method:	Authenticated Only
Authentication:	Windows
NAC/NAM:	No
Edited:	No
QID:	45572
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Patch Available:	No
Virtual Patch Available:	No
Exploitability:	No
Associated Malware:	-
Supported Modules:	Δ Windows Agent



Scan to go to the interactive player