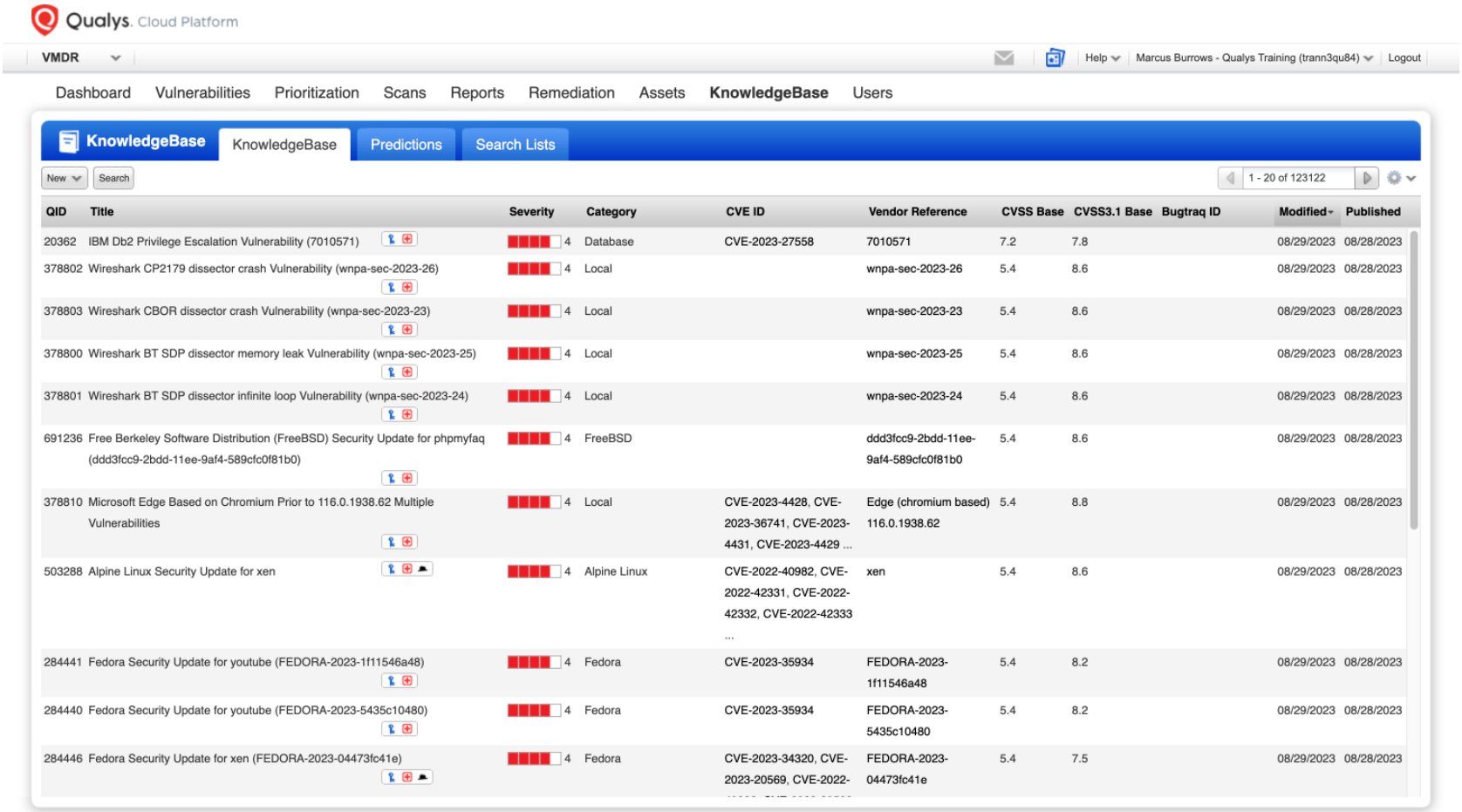
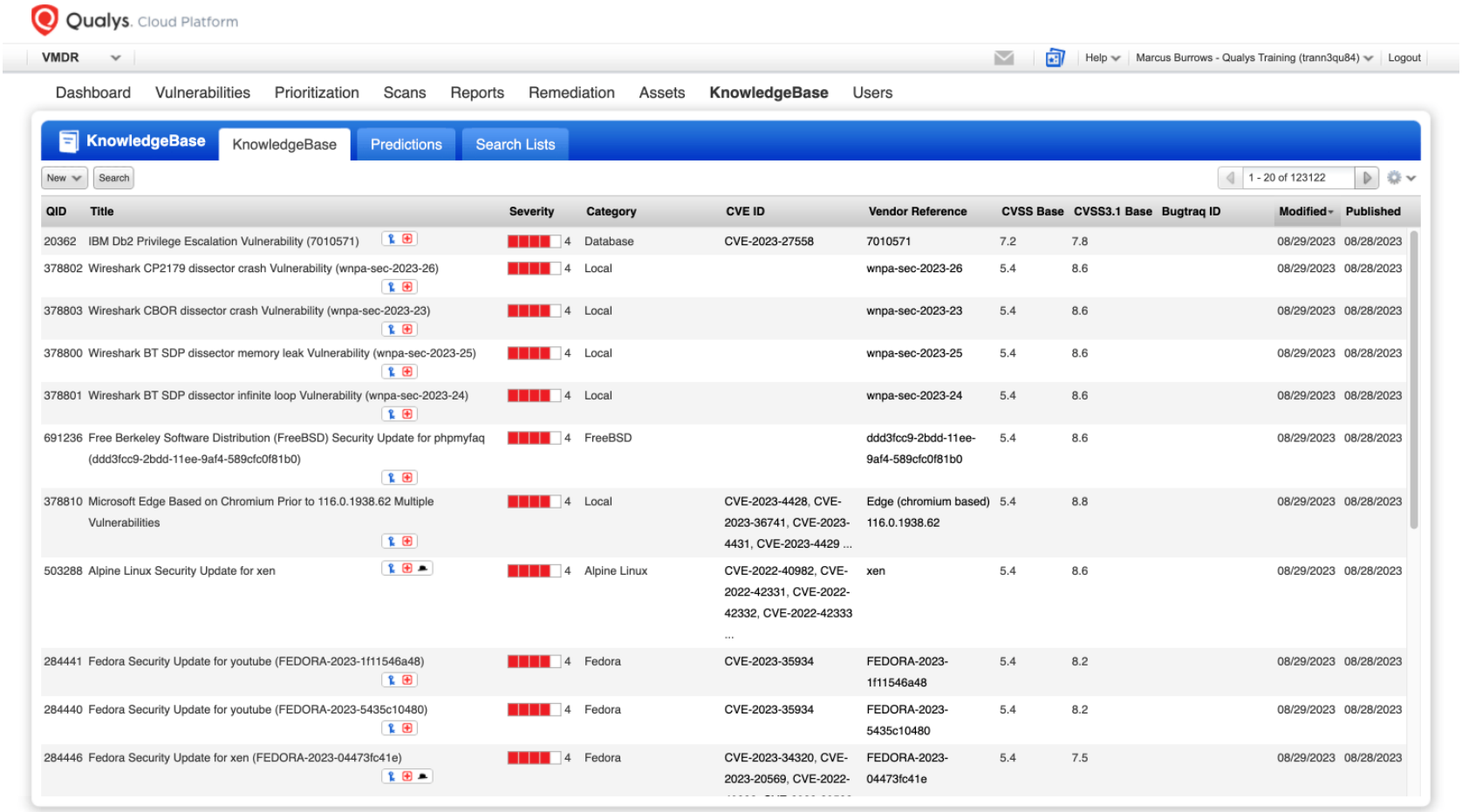
Understanding the Knowledgebase is an important, foundational subject which you need to know before you master other subjects. Can you see how many vulnerabilities are included in total? Click anywhere to continue.



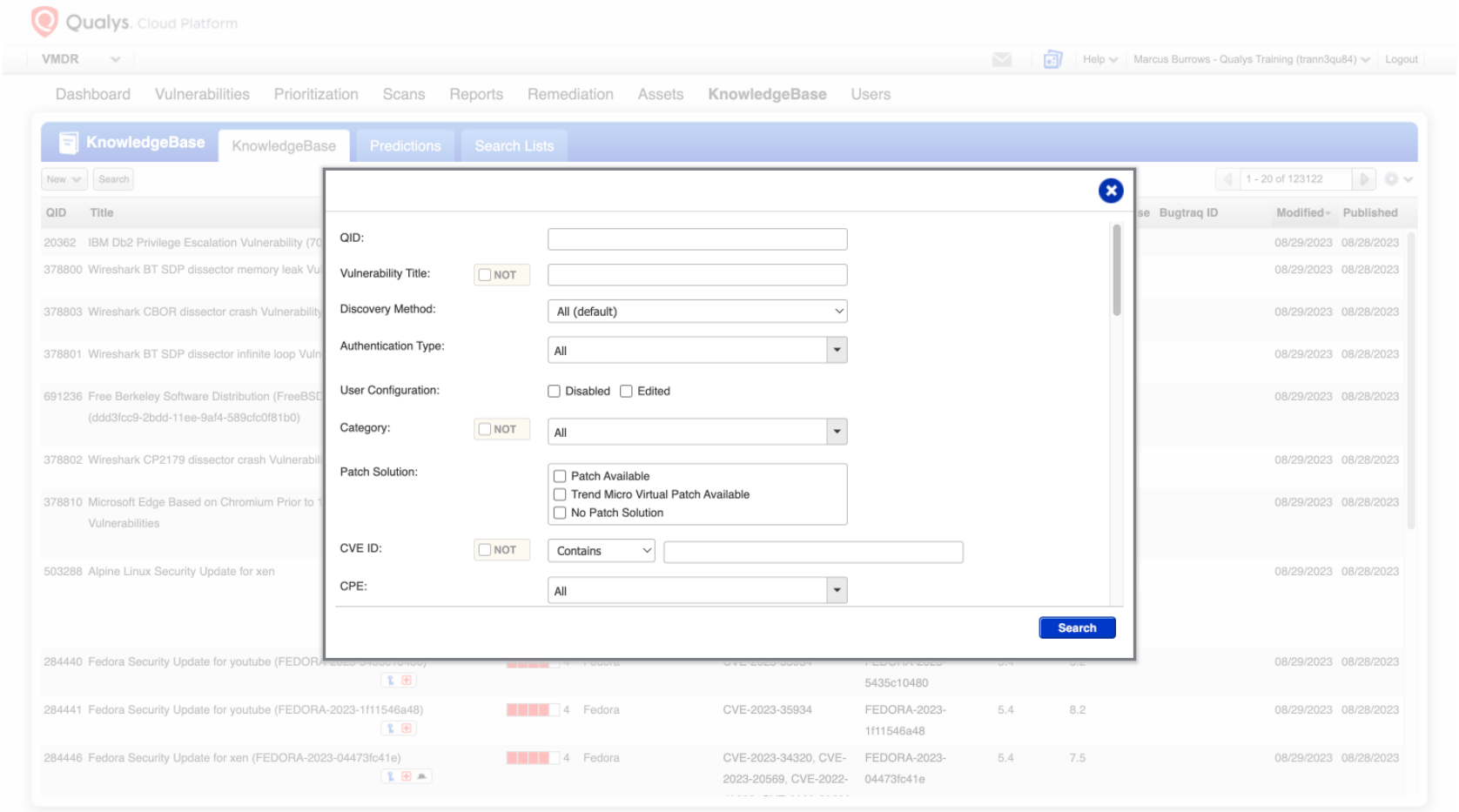
QID	Title	Severity	Category	CVE ID	Vendor Reference	CVSS Base	CVSS3.1 Base	Bugtraq ID	Modified	Published
20362	IBM Db2 Privilege Escalation Vulnerability (7010571)	4	Database	CVE-2023-27558	7010571	7.2	7.8		08/29/2023	08/28/2023
378802	Wireshark CP2179 dissector crash Vulnerability (wnpa-sec-2023-26)	4	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)	4	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)	4	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)	4	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-9af4-589cfc0f81b0)	4	FreeBSD		ddd3fcc9-2bdd-11ee-9af4-589cfc0f81b0	5.4	8.6		08/29/2023	08/28/2023
378810	Microsoft Edge Based on Chromium Prior to 116.0.1938.62 Multiple Vulnerabilities	4	Local	CVE-2023-4428, CVE-2023-36741, CVE-2023-4431, CVE-2023-4429 ...	Edge (chromium based) 116.0.1938.62	5.4	8.8		08/29/2023	08/28/2023
503288	Alpine Linux Security Update for xen	4	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)	4	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)	4	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)	4	Fedora	CVE-2023-34320, CVE-2023-20569, CVE-2022-	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.

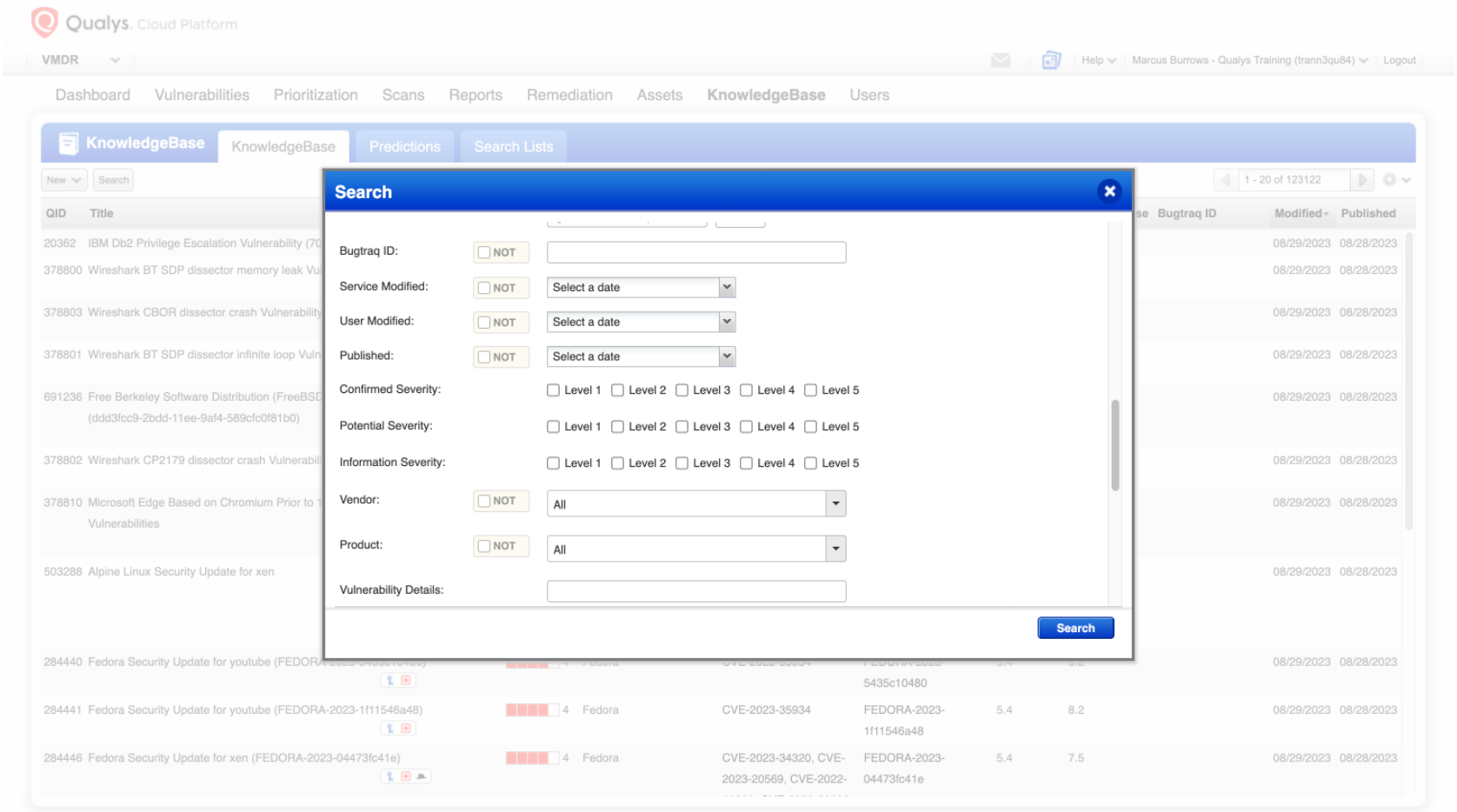


QID	Title	Severity	Category	CVE ID	Vendor Reference	CVSS Base	CVSS3.1 Base	Bugtraq ID	Modified	Published
20362	IBM Db2 Privilege Escalation Vulnerability (7010571)	4	Database	CVE-2023-27558	7010571	7.2	7.8		08/29/2023	08/28/2023
378802	Wireshark CP2179 dissector crash Vulnerability (wnpa-sec-2023-26)	4	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)	4	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)	4	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)	4	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-9af4-589cfc0f81b0)	4	FreeBSD		ddd3fcc9-2bdd-11ee-9af4-589cfc0f81b0	5.4	8.6		08/29/2023	08/28/2023
378810	Microsoft Edge Based on Chromium Prior to 116.0.1938.62 Multiple Vulnerabilities	4	Local	CVE-2023-4428, CVE-2023-36741, CVE-2023-4431, CVE-2023-4429 ...	Edge (chromium based) 116.0.1938.62	5.4	8.8		08/29/2023	08/28/2023
503288	Alpine Linux Security Update for xen	4	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)	4	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)	4	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)	4	Fedora	CVE-2023-34320, CVE-2023-20569, CVE-2022-	FEDORA-2023-04473fc41e	5.4	7.5		08/29/2023	08/28/2023

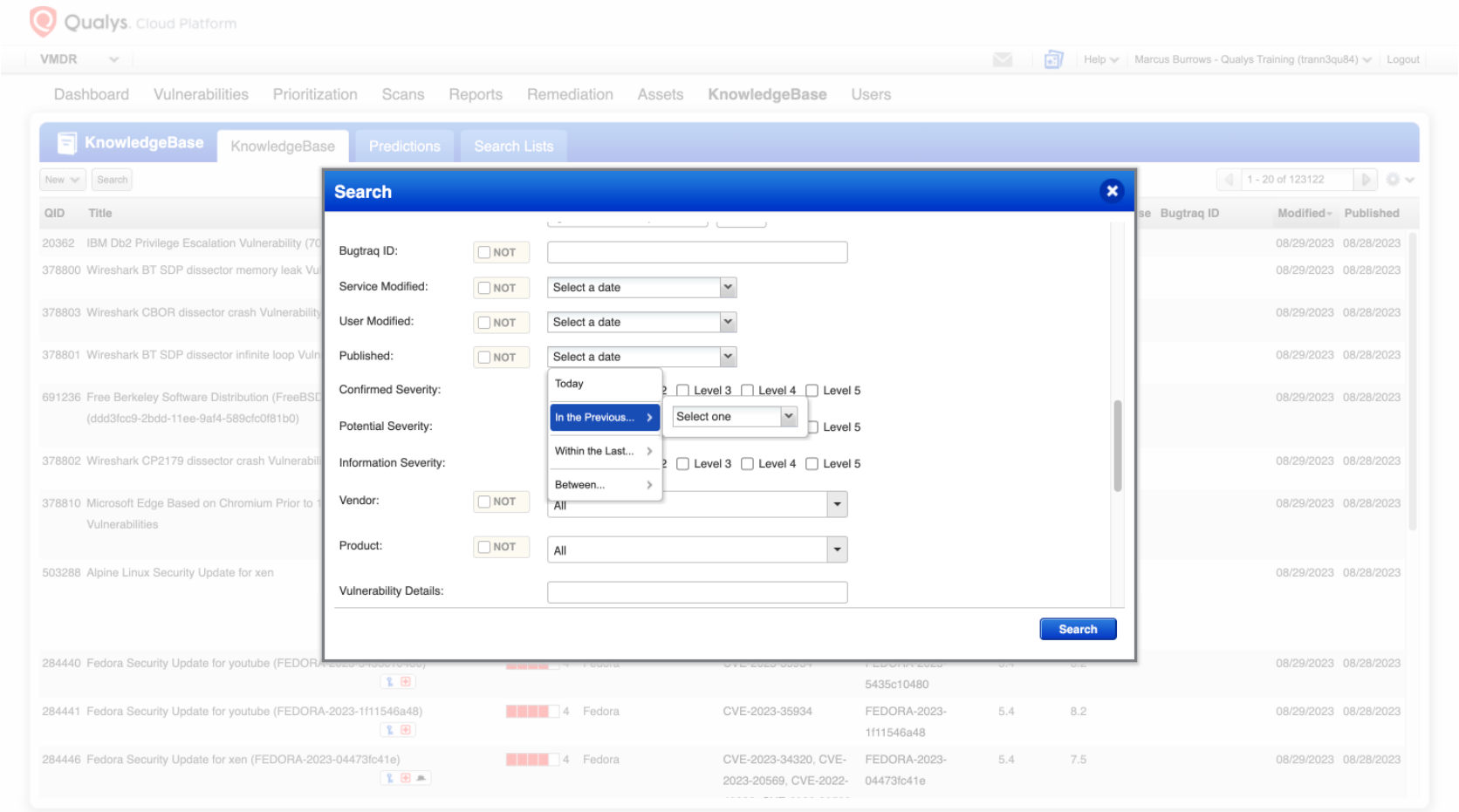
In the Search dialog box, click on the scroll bar to scroll down.



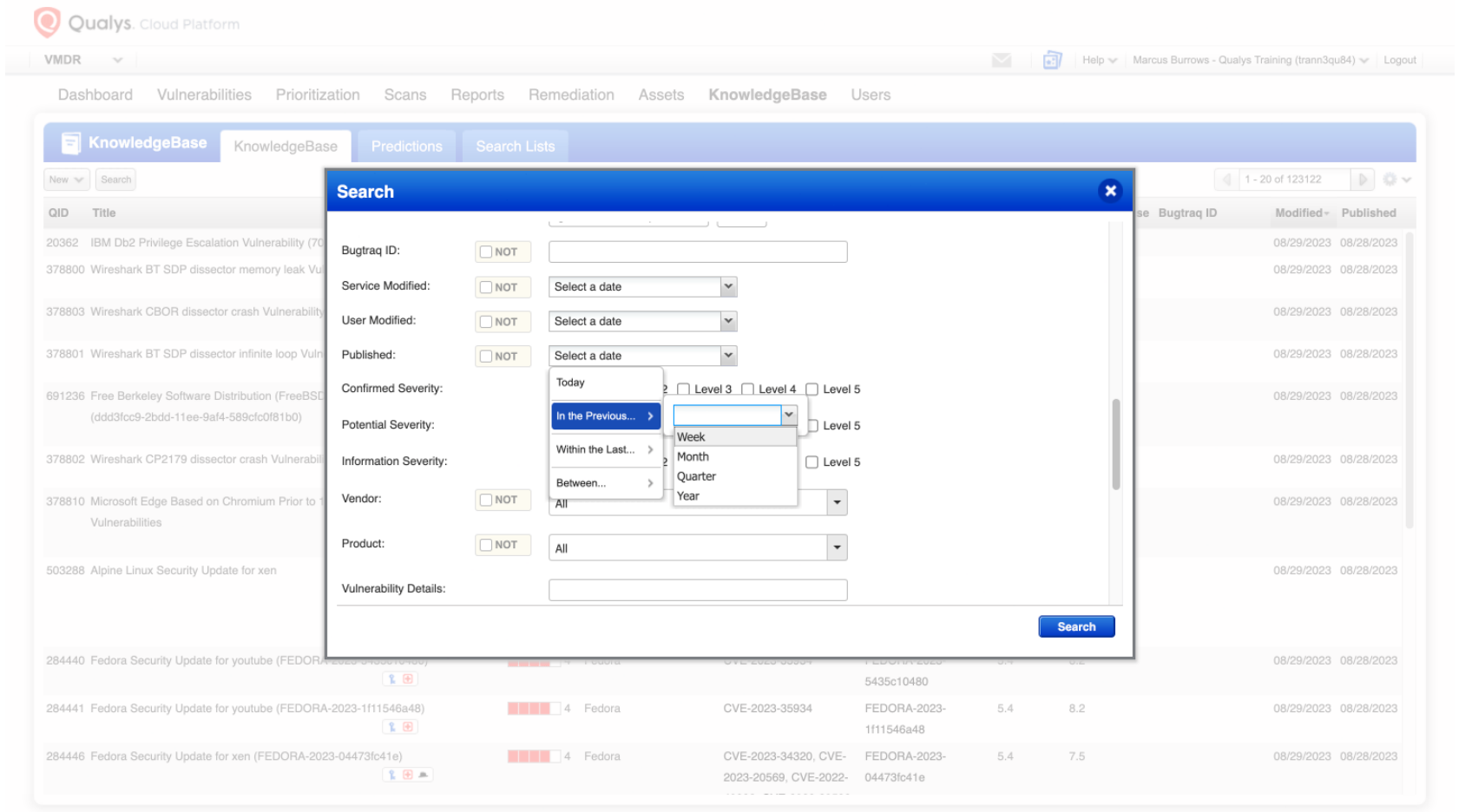
You are now going to filter the knowledgebase to only those entries published in the previous month. Click on the drop down arrow next to "Published".



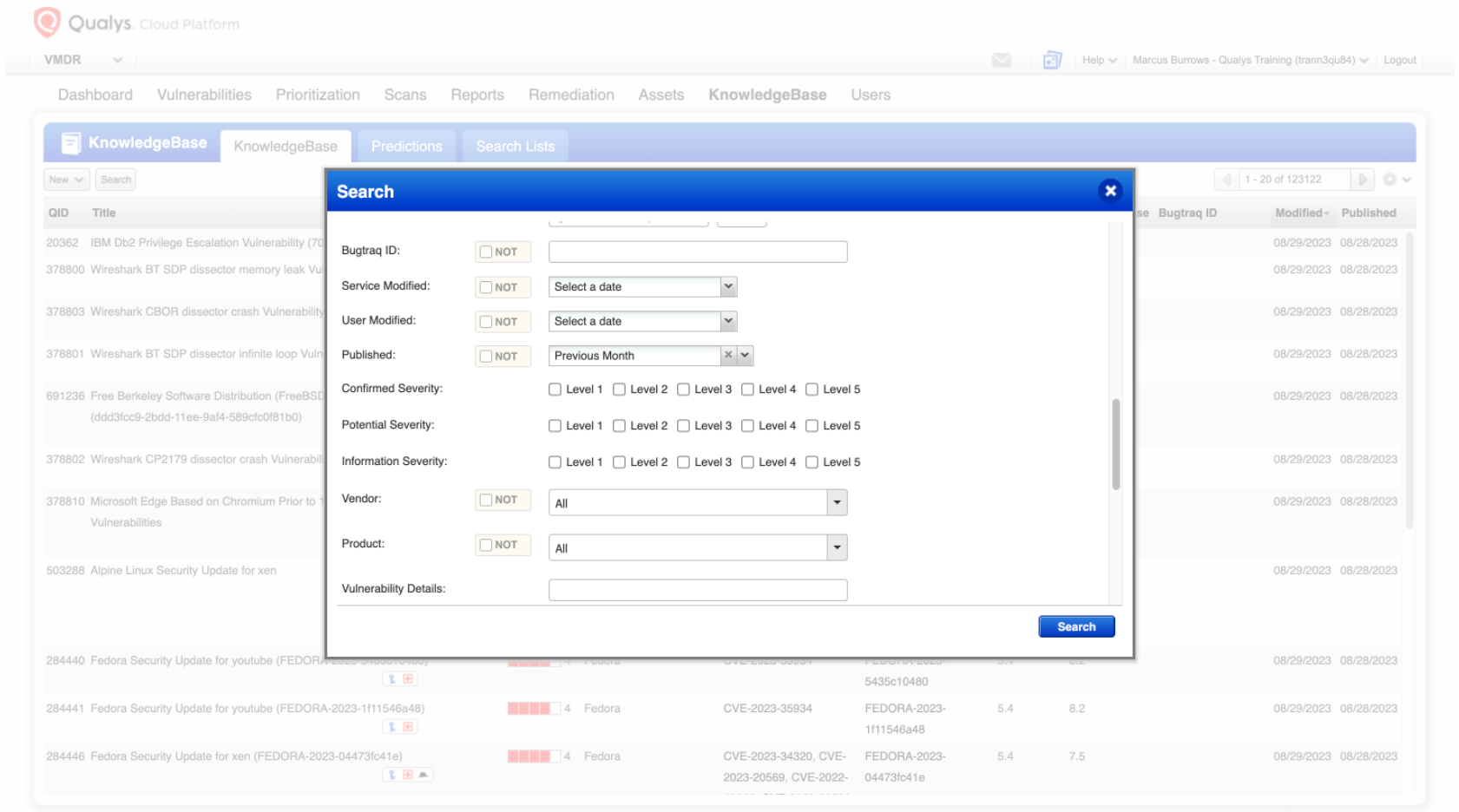
Click the drop down arrow to select a time range.



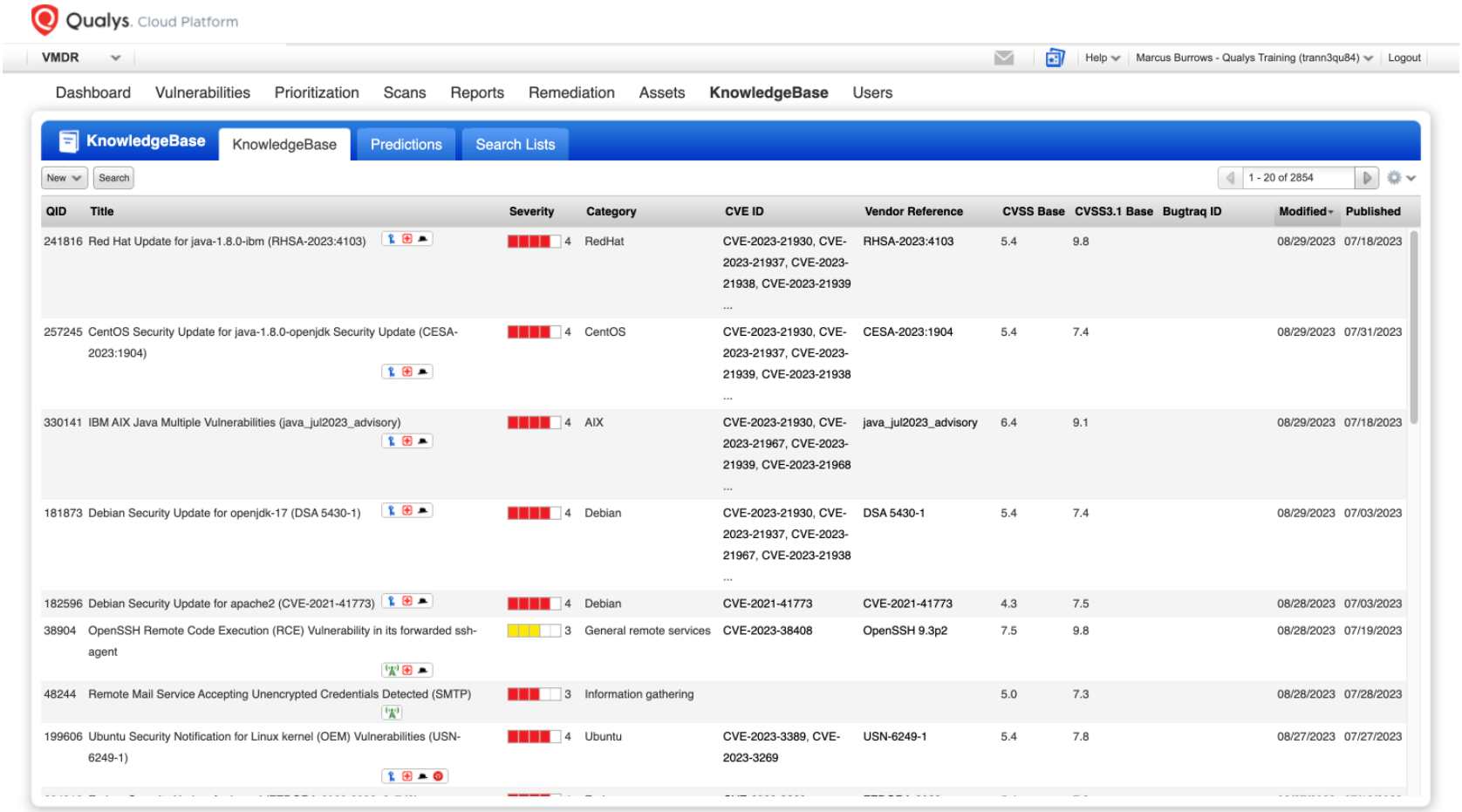
Click Month


Qualys. Cloud Platform
VMDR
Help
Marcus Burrows - Qualys Training (trann3qu84)
Logout
Dashboard
Vulnerabilities
Prioritization
Scans
Reports
Remediation
Assets
KnowledgeBase
Users
KnowledgeBase
KnowledgeBase
Predictions
Search Lists
New
Search
1 - 20 of 123122
QID
Title
Bugtraq ID
Modified
Published
Search
Bugtraq ID:
Service Modified:
User Modified:
Published:
Confirmed Severity:
Potential Severity:
Information Severity:
Vendor:
Product:
Vulnerability Details:
NOT
Select a date
Level 3
Level 4
Level 5
Today
In the Previous...
Within the Last...
Between...
Week
Month
Quarter
Year
All
Search

Click the Search button

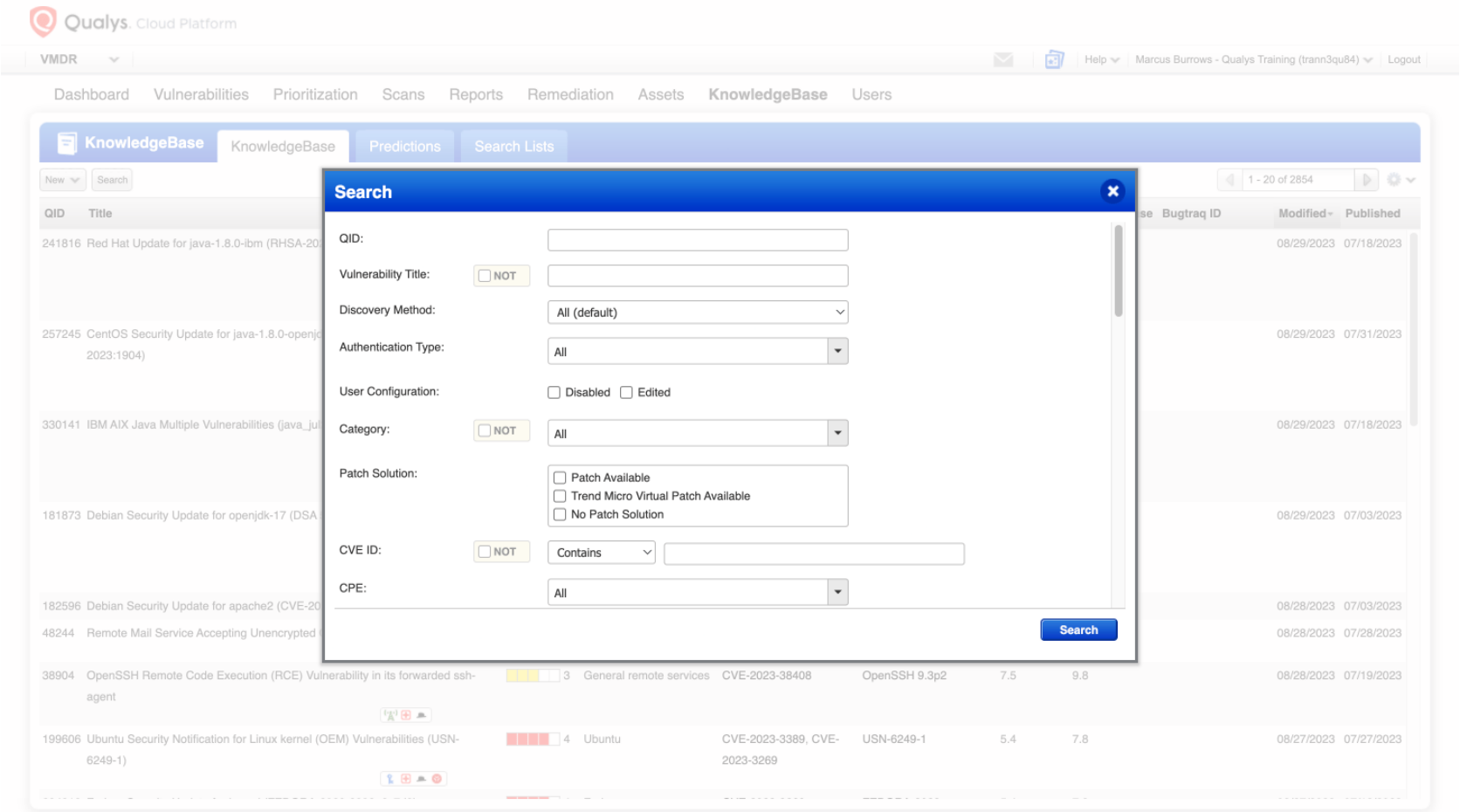


Notice how the number of vulnerabilities that are displayed has been reduced. Click on the Search button again to filter the list even further.

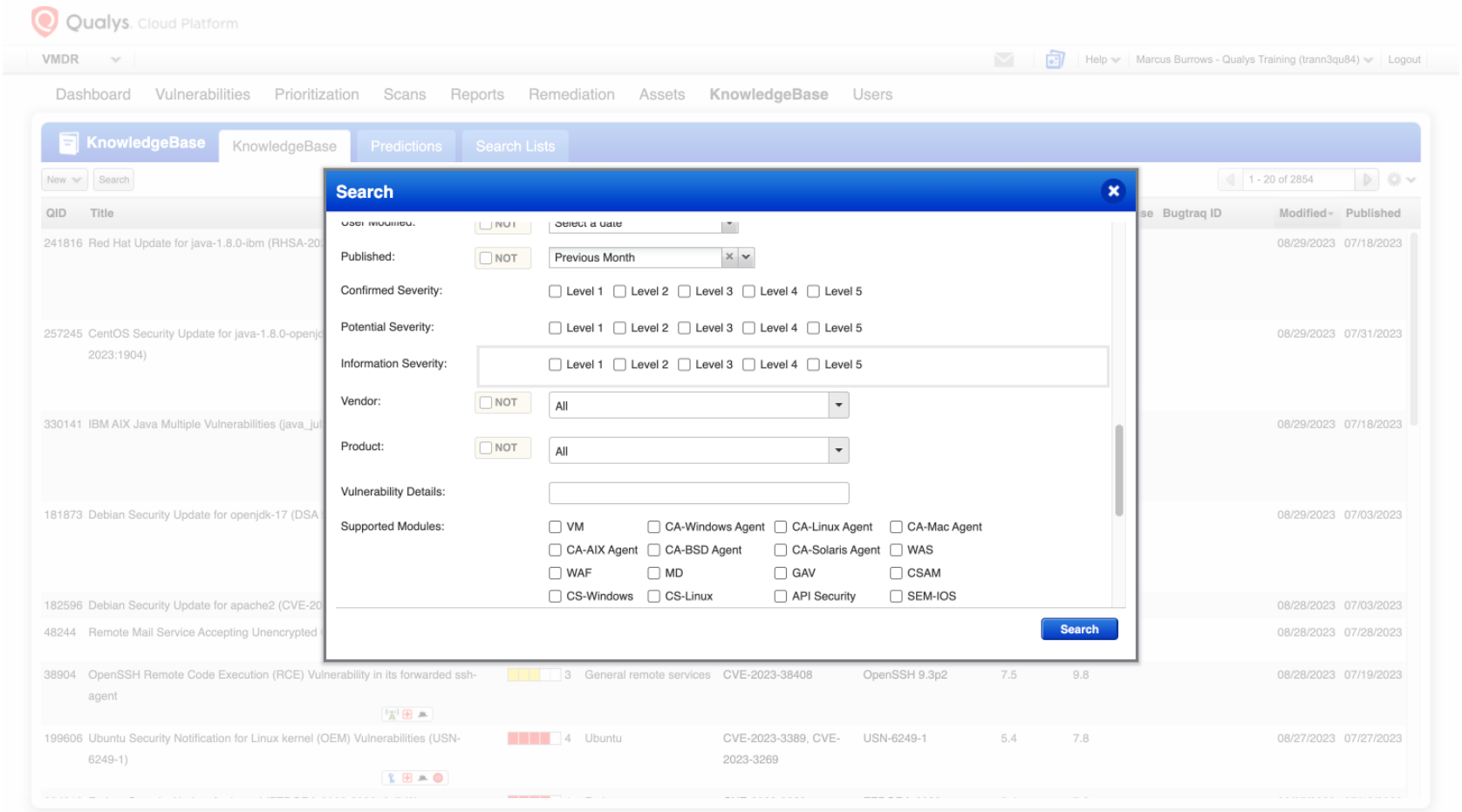


QID	Title	Severity	Category	CVE ID	Vendor Reference	CVSS Base	CVSS3.1 Base	Bugtraq ID	Modified	Published
241816	Red Hat Update for java-1.8.0-ibm (RHSA-2023:4103)	4	RedHat	CVE-2023-21930, CVE-2023-21937, CVE-2023-21938, CVE-2023-21939 ...	RHSA-2023:4103	5.4	9.8		08/29/2023	07/18/2023
257245	CentOS Security 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

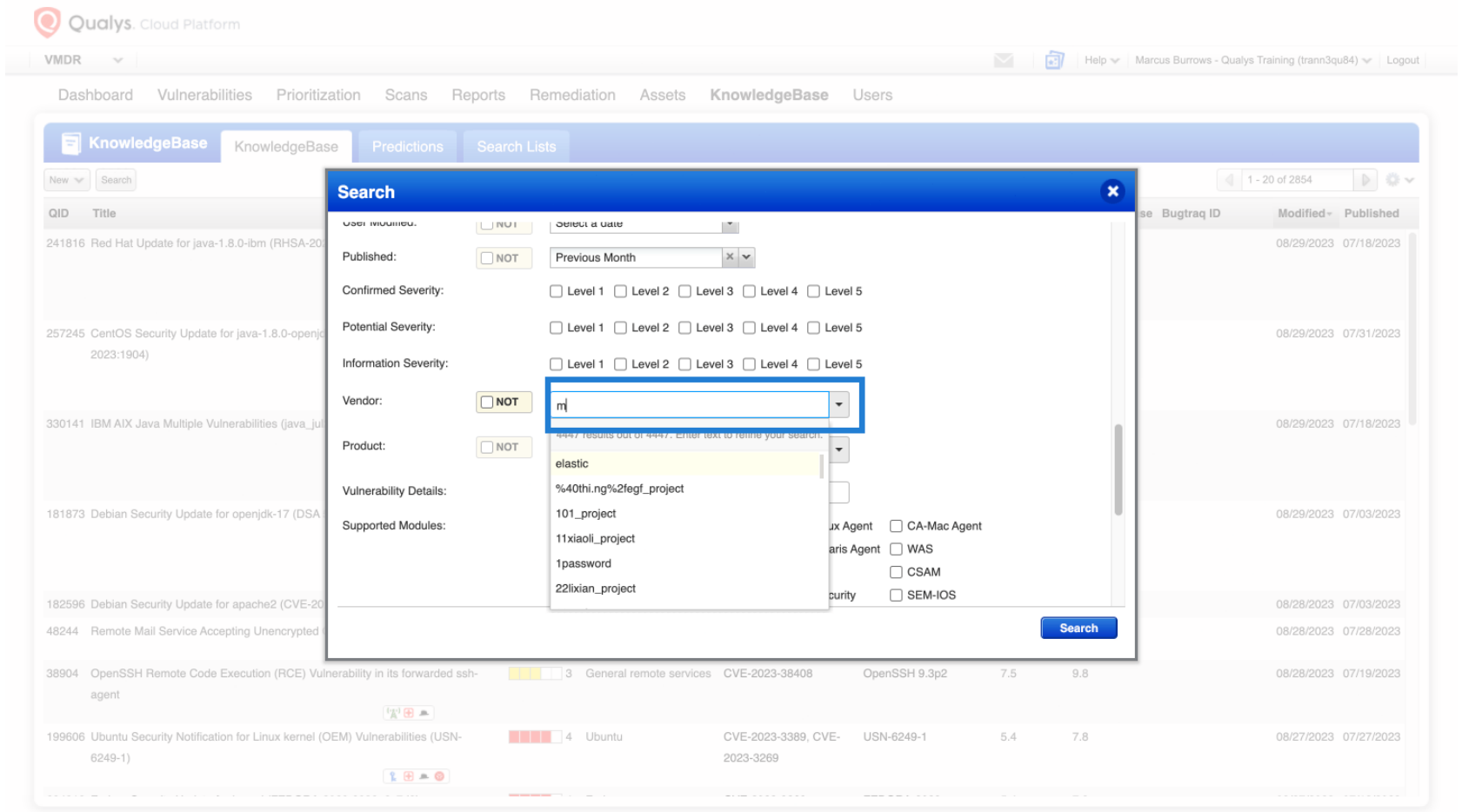
In the Search dialog box, click the scroll bar to scroll down.



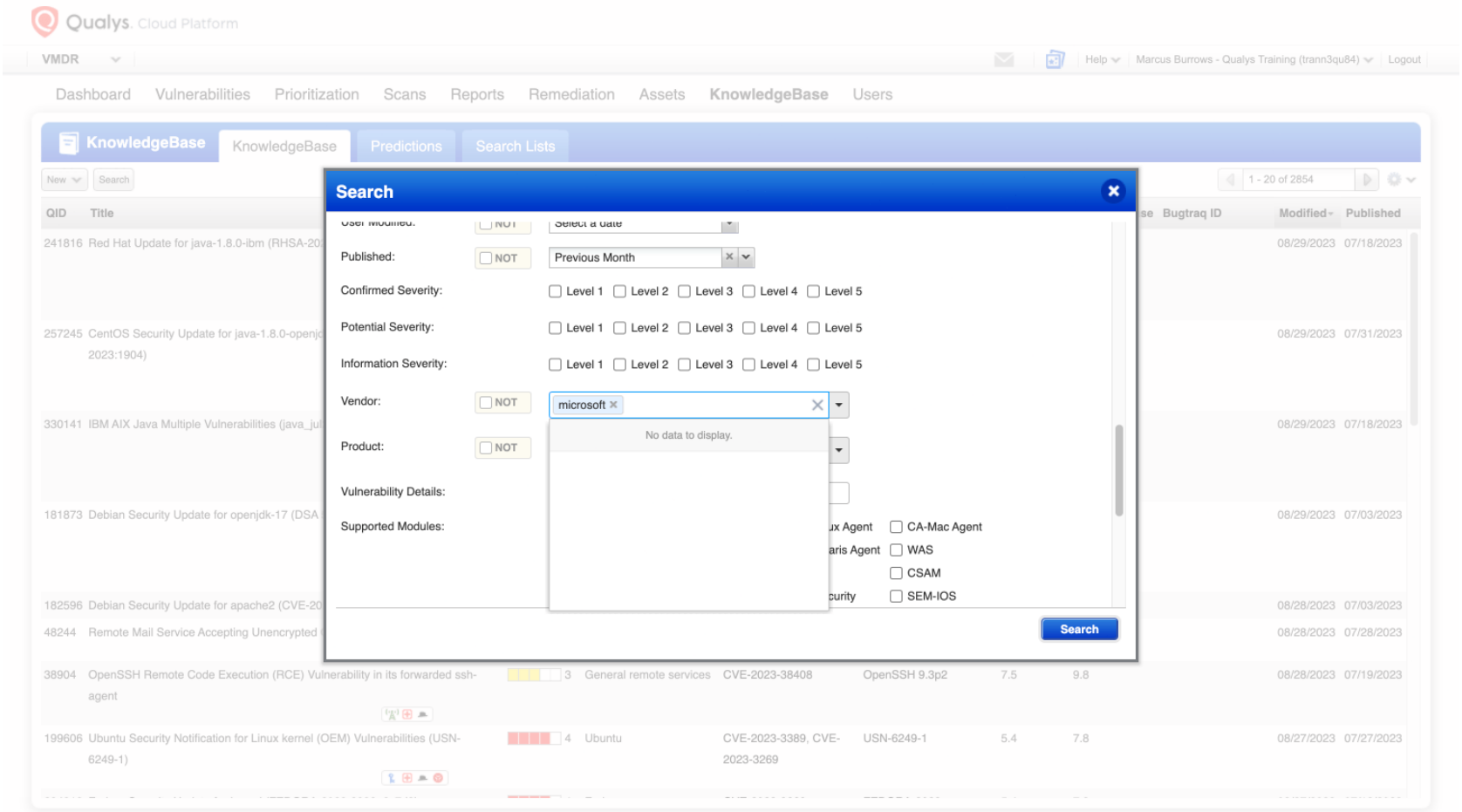
Click the drop down arrow next to Vendor



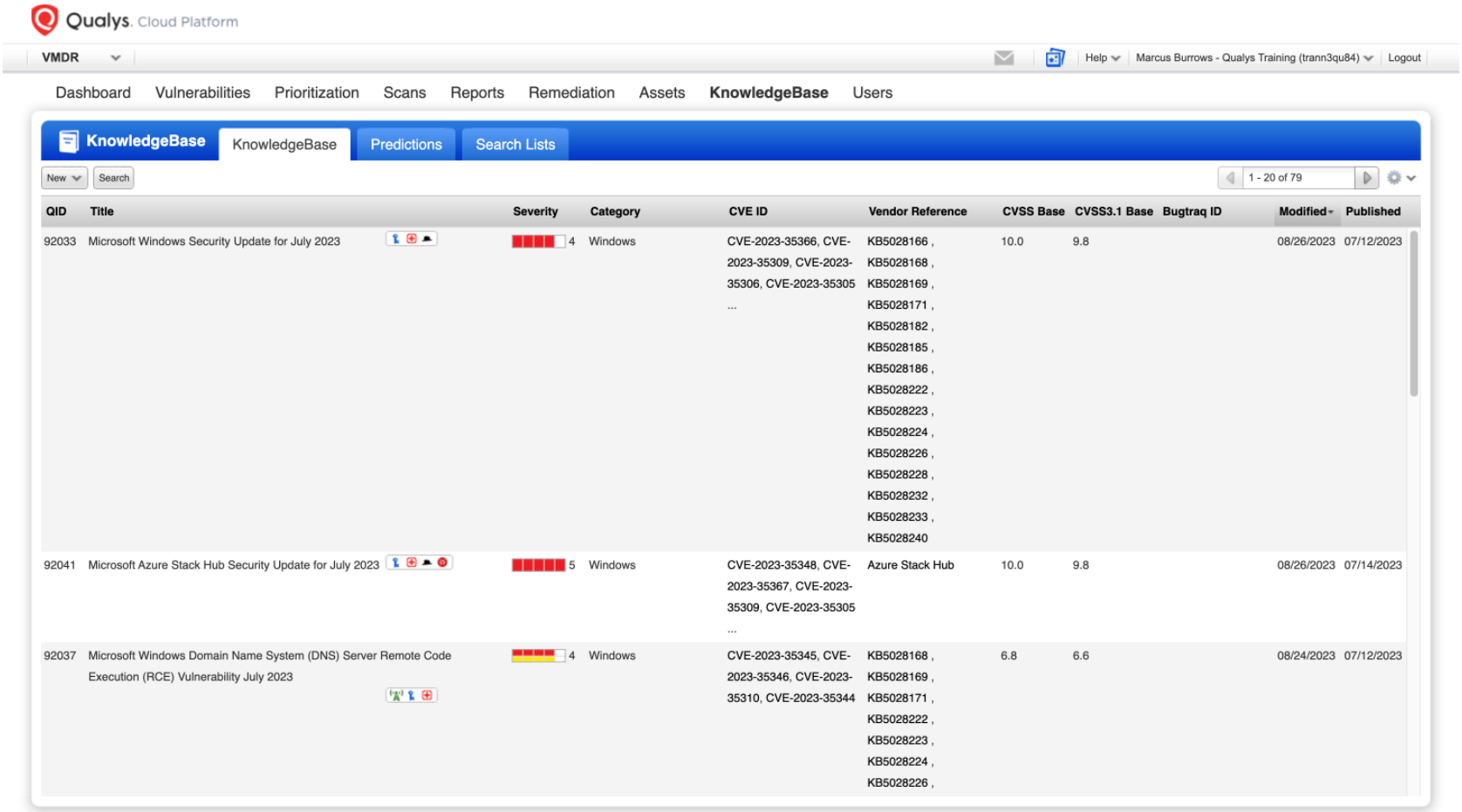
Type microsoft



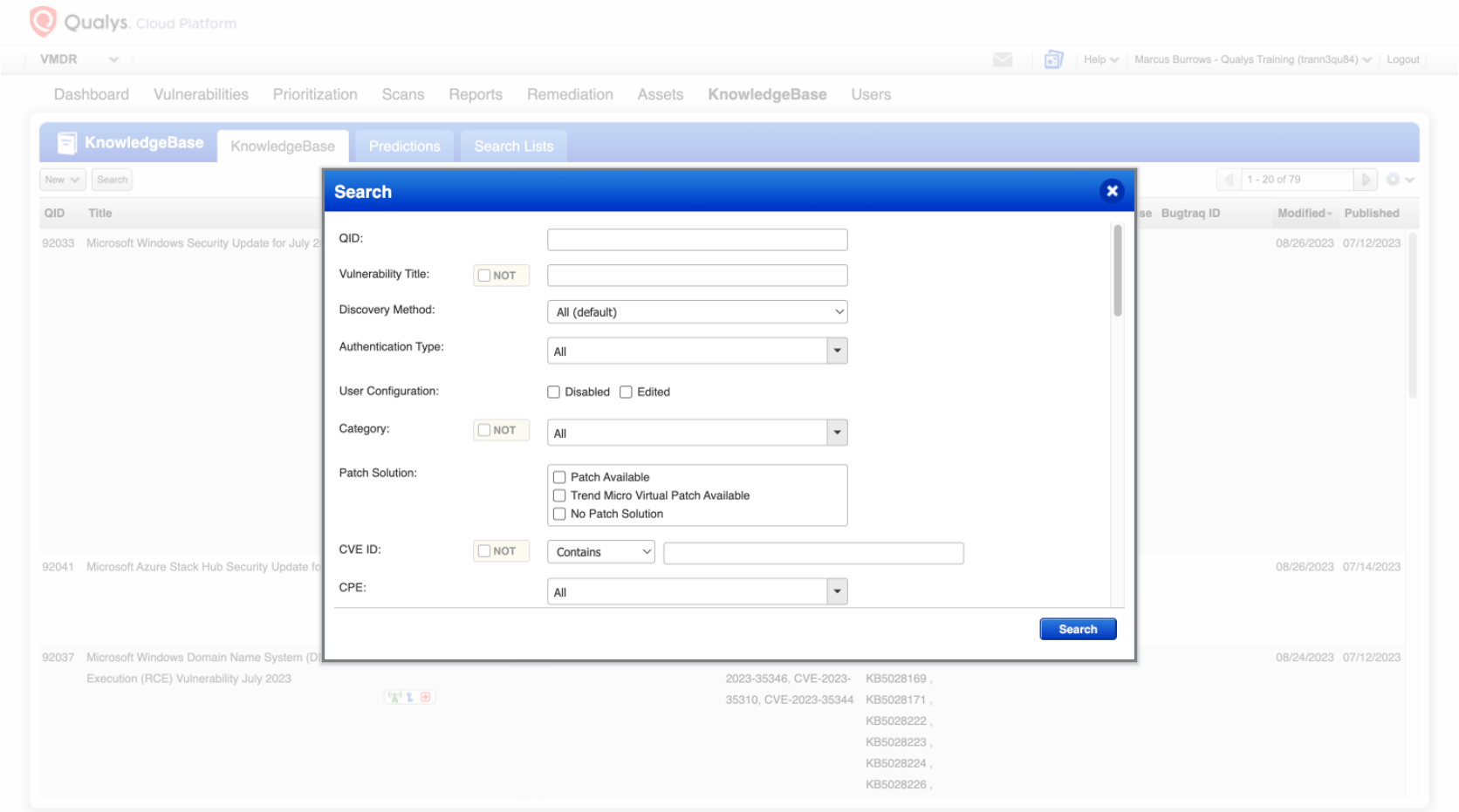
Click the Search button.



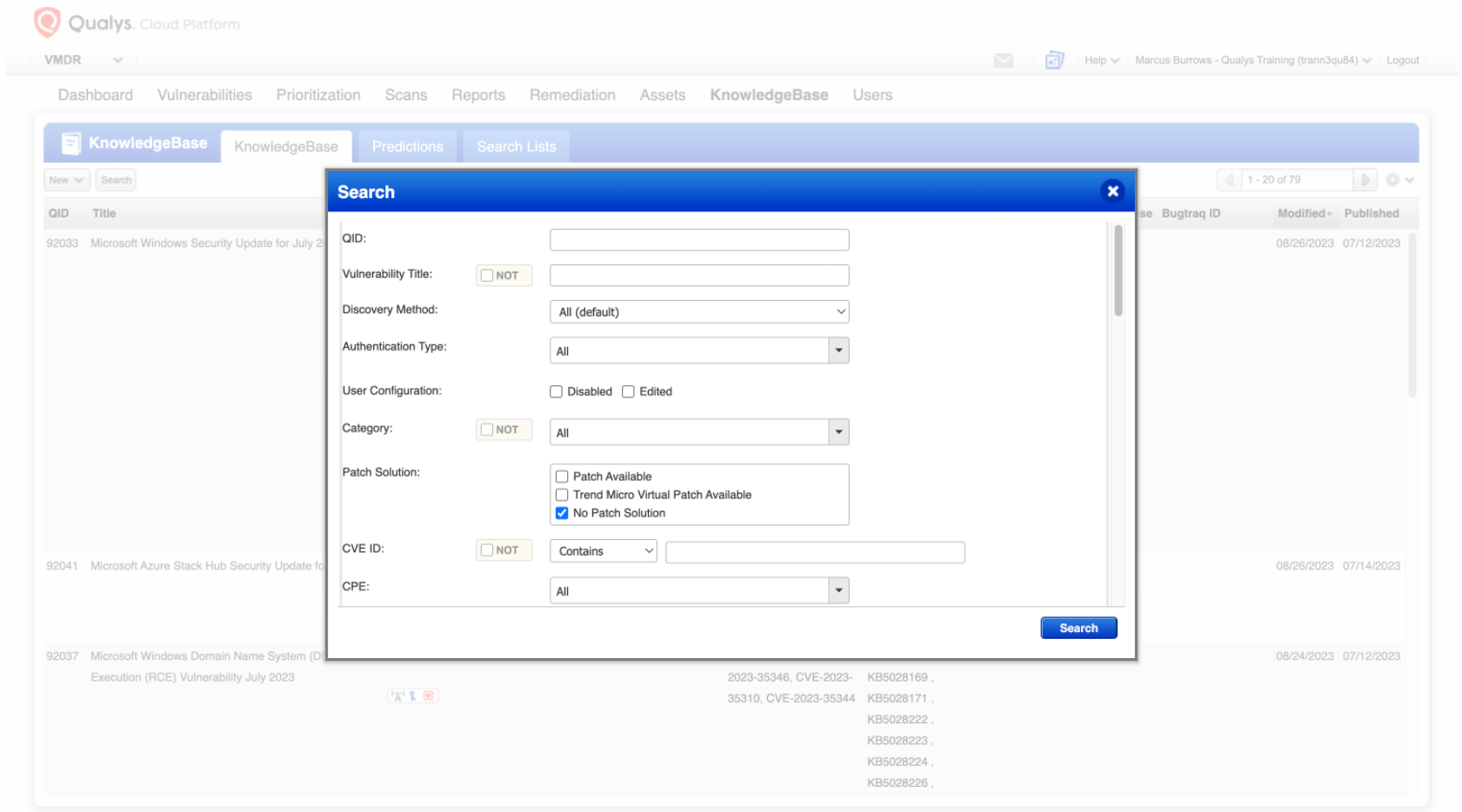
Notice how the total number of vulnerabilities has again been reduced. Next, click on the Search button again to filter the list even further.



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

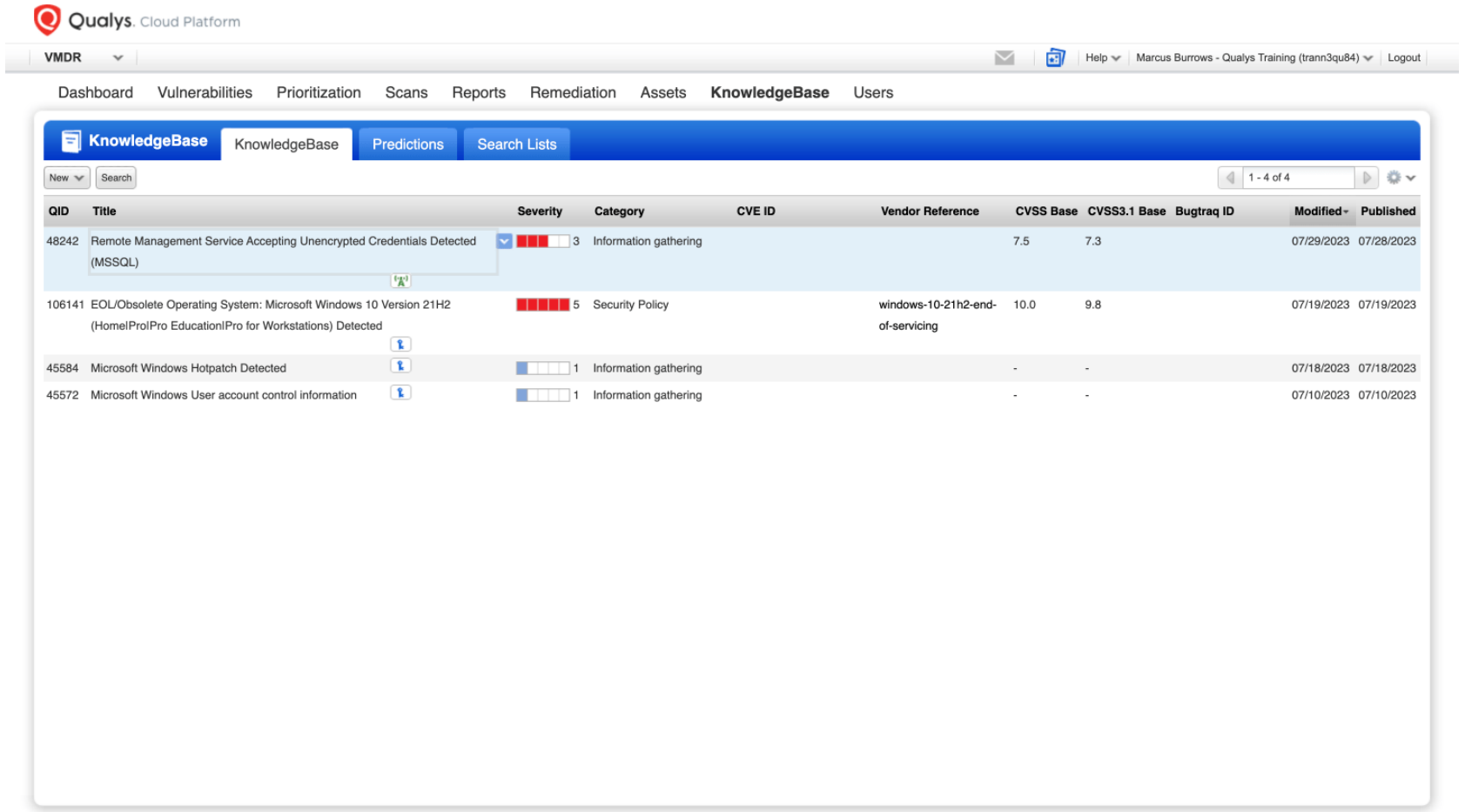


Click Search

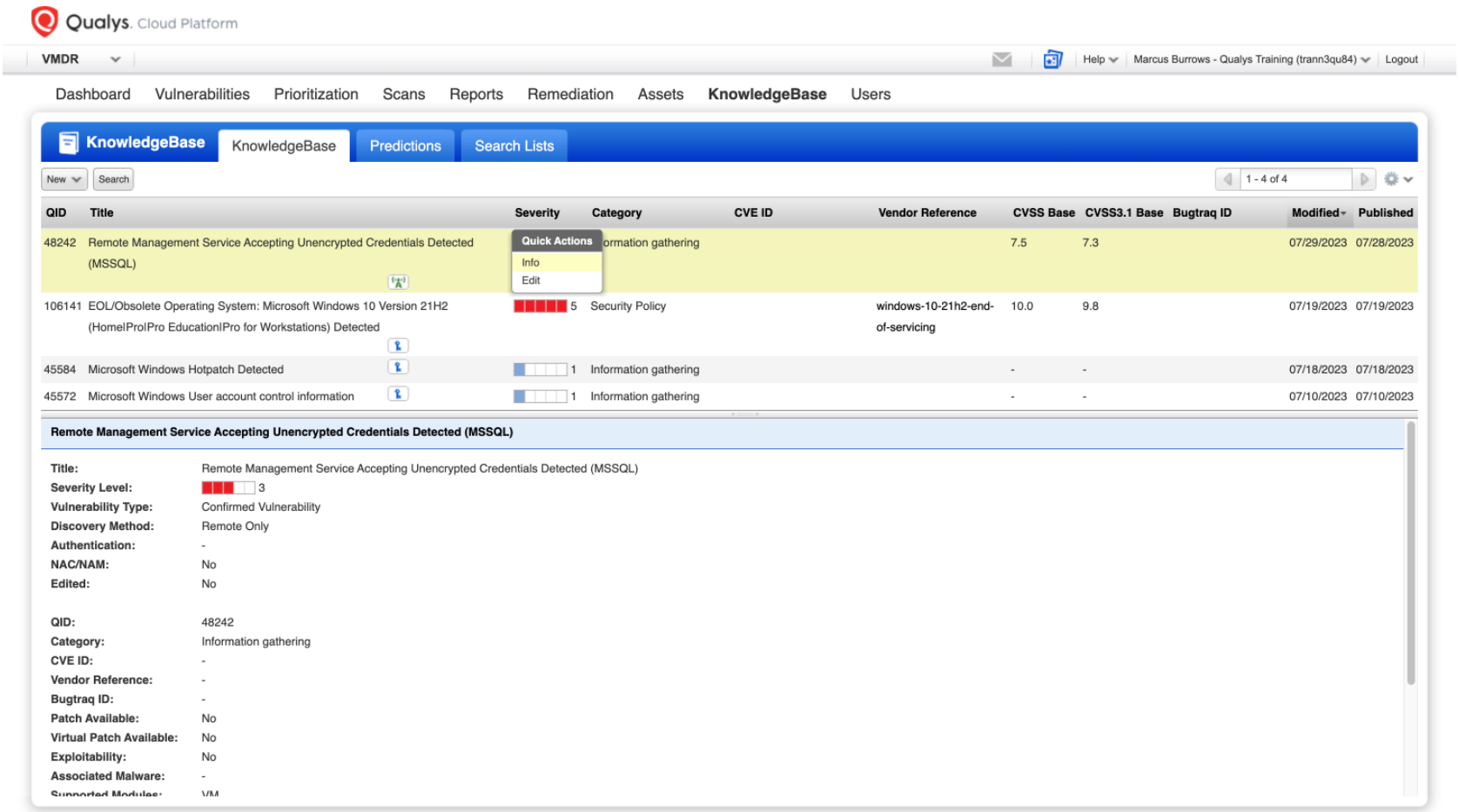


You have filtered the list to show only Microsoft vulnerabilities that have been published within the last month, and which have no patch solution available. Click on the drop down arrow next to the first vulnerability in order to see more details.

Understanding the Vulnerability Knowledgebase

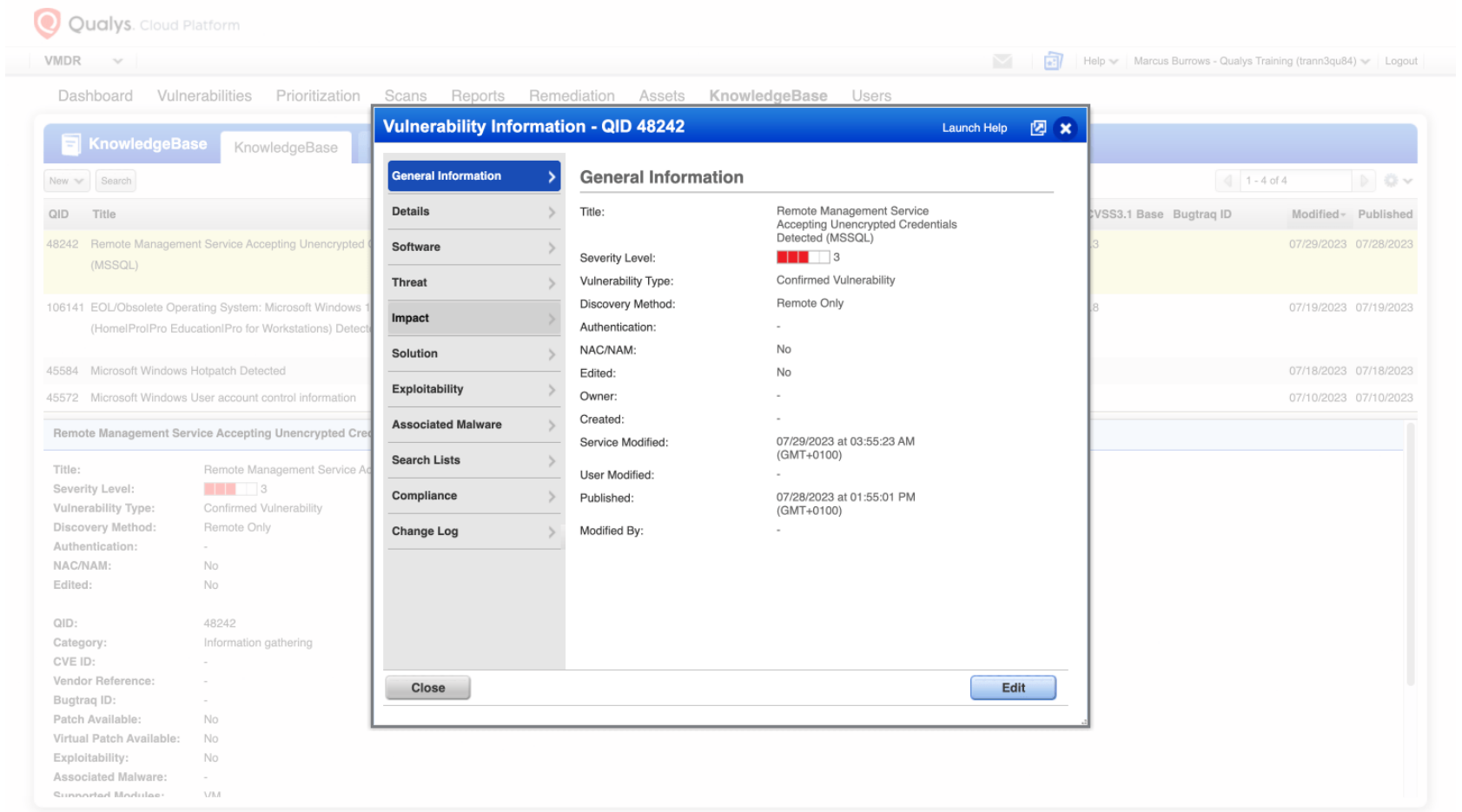


Click Info

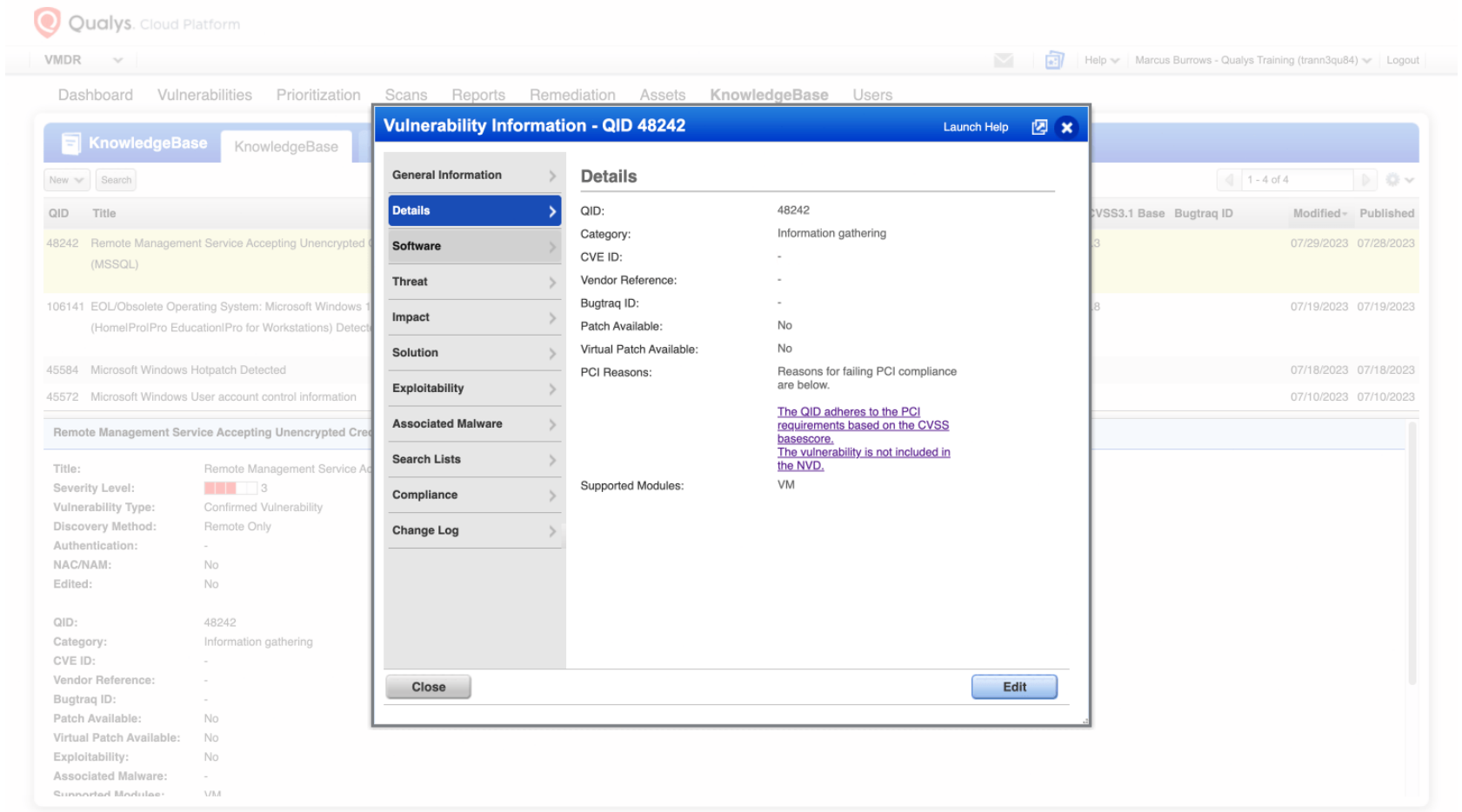

Qualys. Cloud Platform
VMDR
Help
Marcus Burrows - Qualys Training (trann3qu84)
Logout
Dashboard
Vulnerabilities
Prioritization
Scans
Reports
Remediation
Assets
KnowledgeBase
Users
KnowledgeBase
KnowledgeBase
Predictions
Search Lists
New
Search
1 - 4 of 4
QID
Title
Severity
Category
CVE ID
Vendor Reference
CVSS Base
CVSS3.1 Base
Bugtraq ID
Modified
Published
48242
Remote Management Service Accepting Unencrypted Credentials Detected (MSSQL)
Quick Actions
Info
Edit
ormation gathering
7.5
7.3
07/29/2023
07/28/2023
106141
EOL/Obsolete Operating System: Microsoft Windows 10 Version 21H2 (HomeIProIPro EducationIPro 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)
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:
-

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.

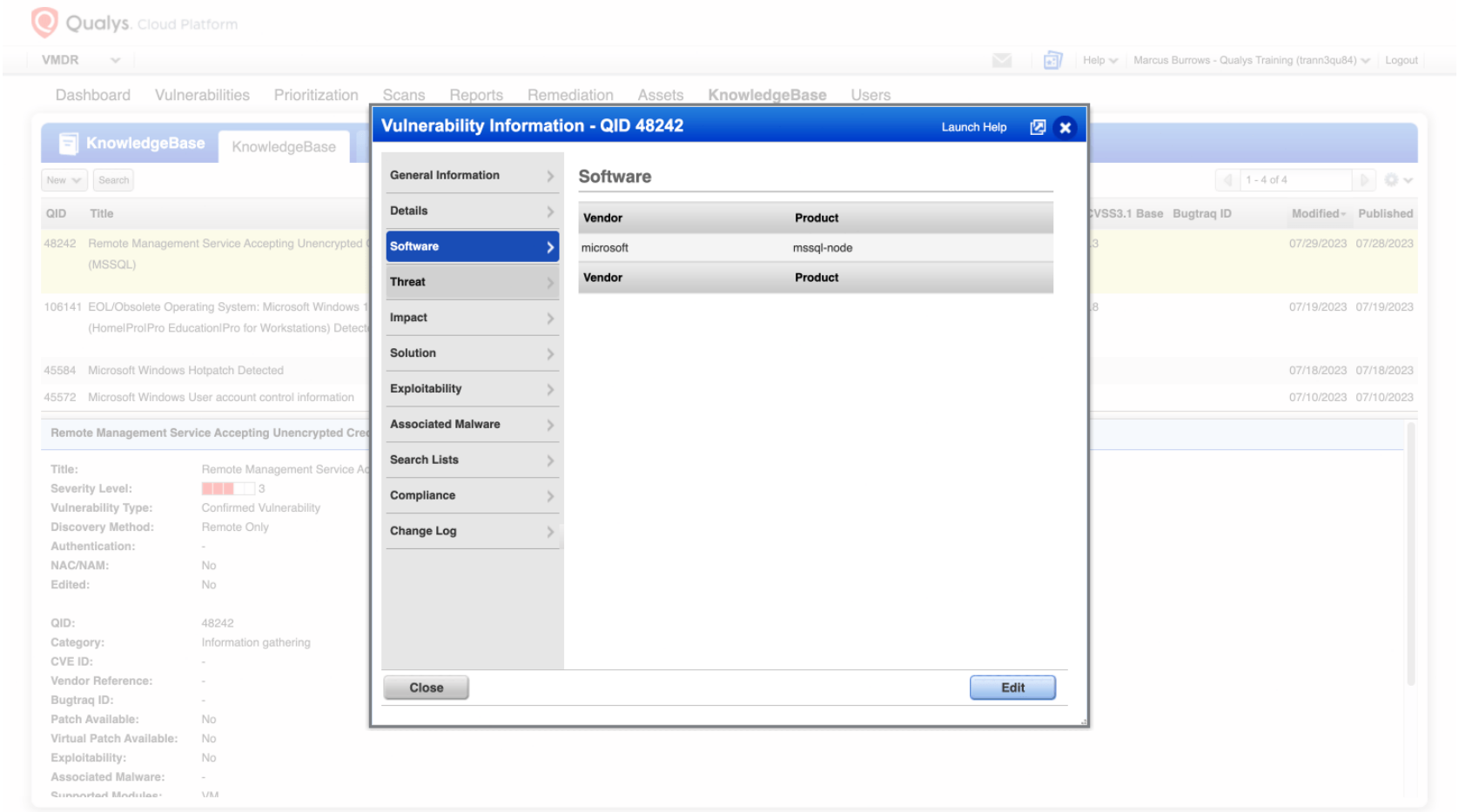
Understanding the Vulnerability Knowledgebase



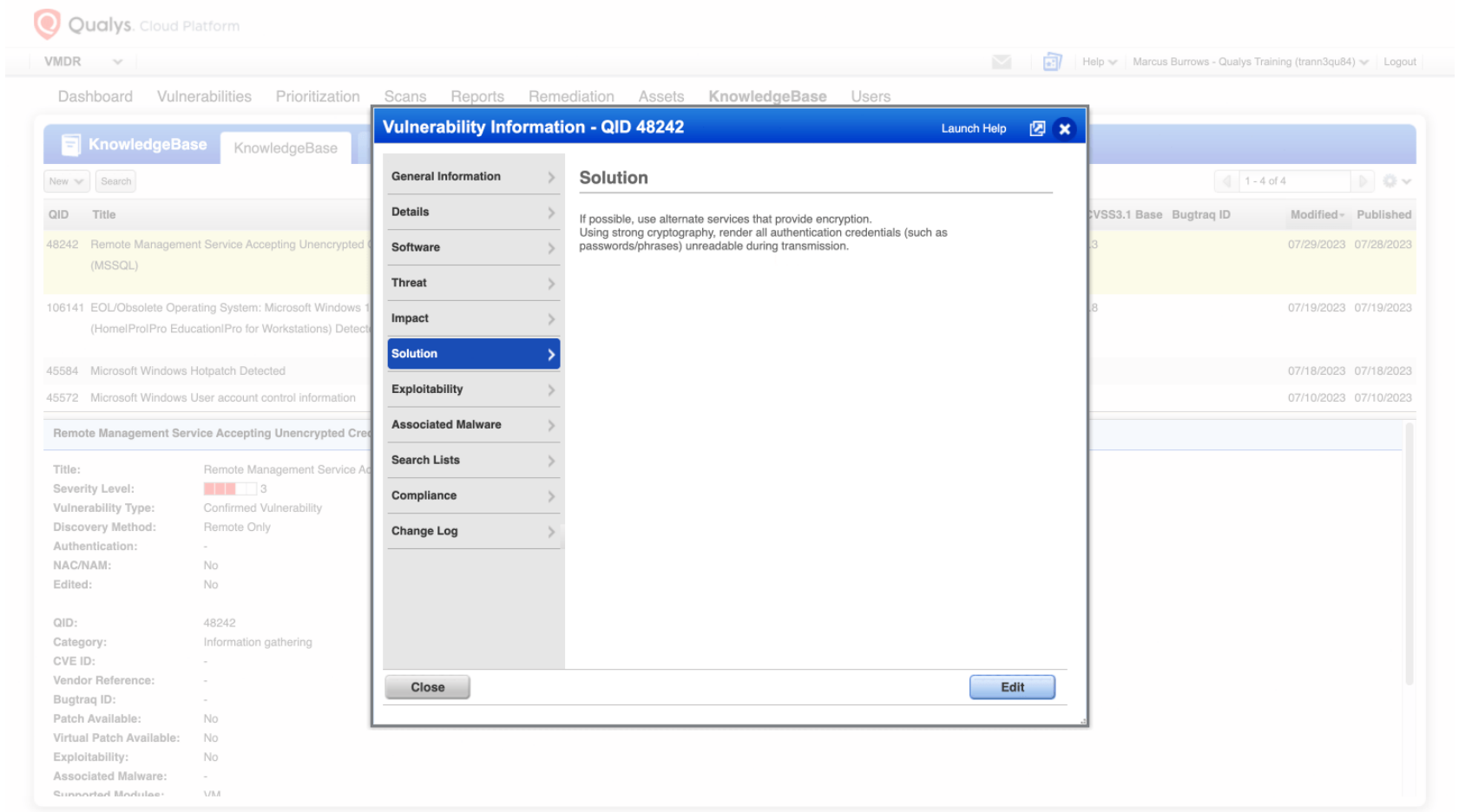
The details tab displays CVE and vendor references, where applicable. Click on the Software tab to continue.



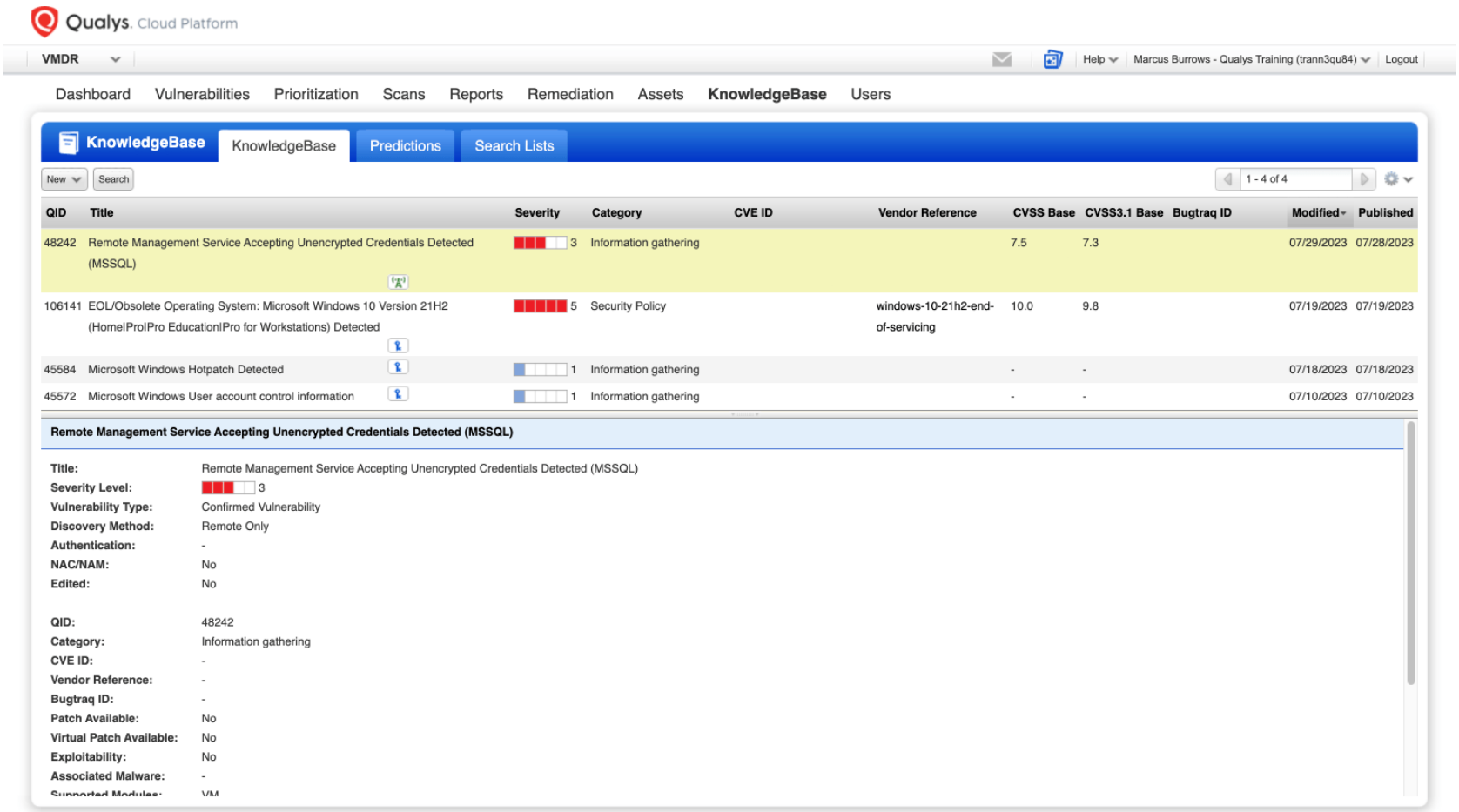
In the Software tab, we can see the vendor and product to which this vulnerability refers. Click the Solution tab to continue.



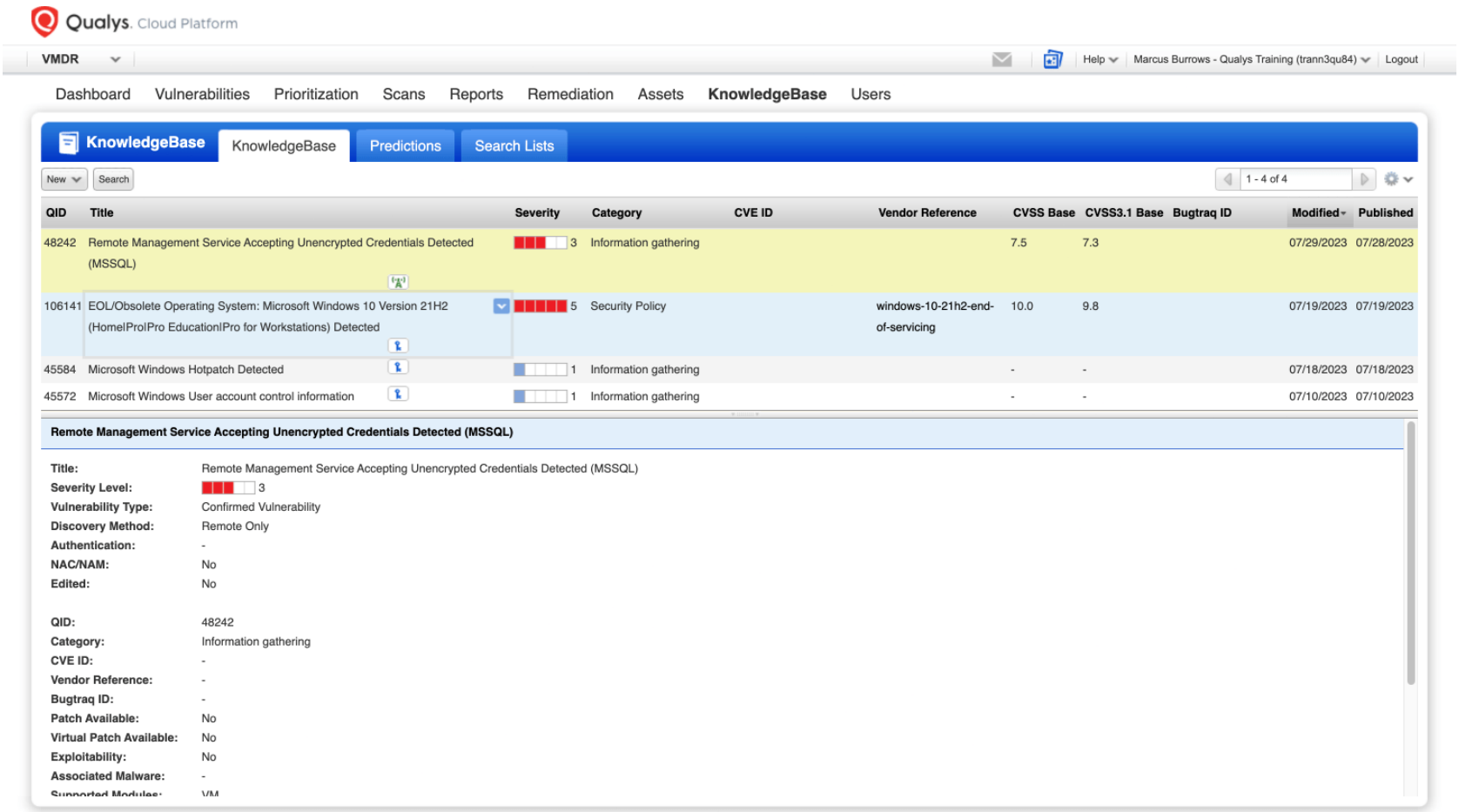
Sometimes the Solution tab will display patch details. There is no relevant patch for this vulnerability, but a recommended action is given instead. Click the Close button.



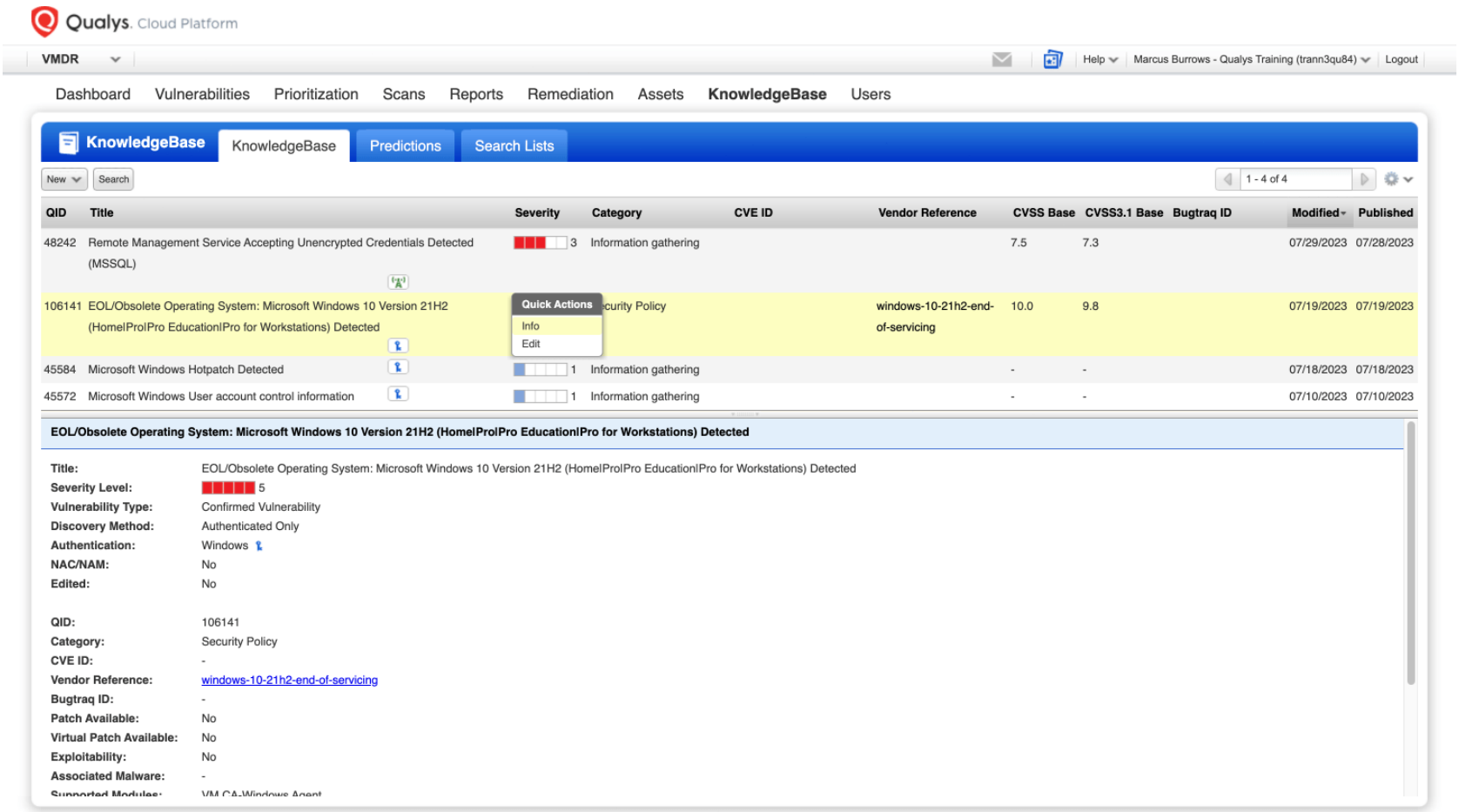
Click the second vulnerability in the list to continue.



Click the drop down arrow next to the second vulnerability.

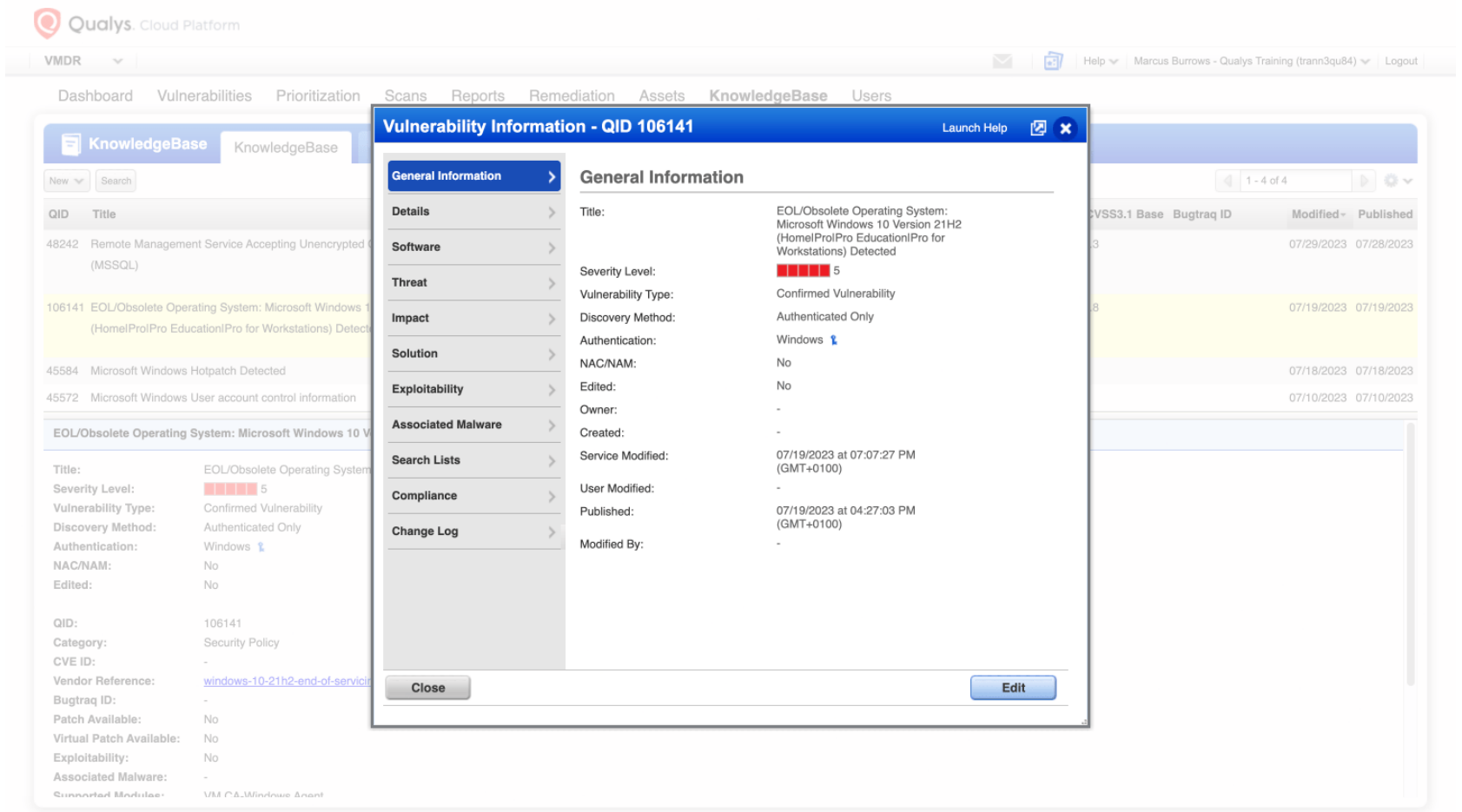


Click Info

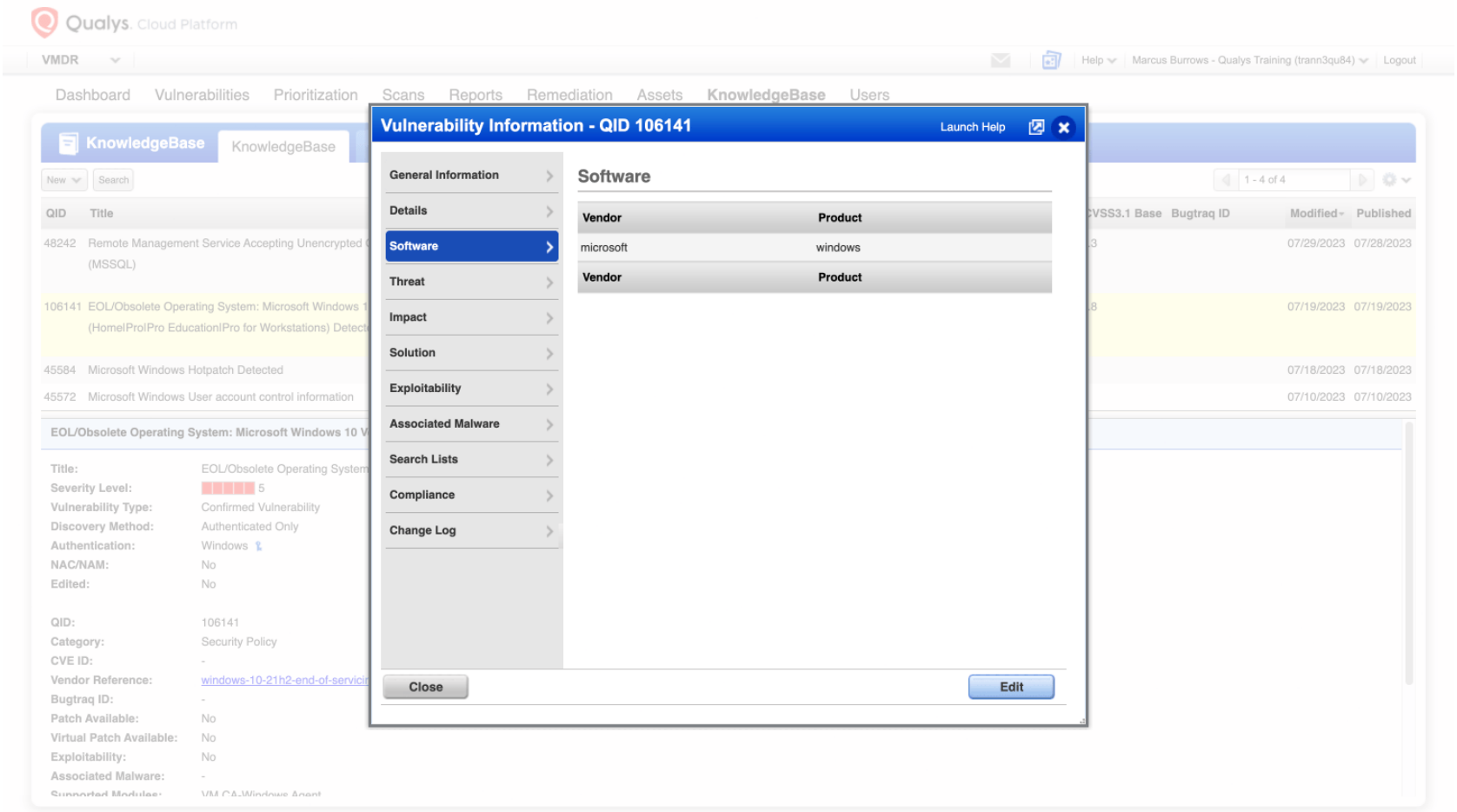

Qualys. Cloud Platform
VMDR
Help
Marcus Burrows - Qualys Training (trann3qu84)
Logout
Dashboard
Vulnerabilities
Prioritization
Scans
Reports
Remediation
Assets
KnowledgeBase
Users
KnowledgeBase
KnowledgeBase
Predictions
Search Lists
New
Search
1 - 4 of 4
QID
Title
Severity
Category
CVE ID
Vendor Reference
CVSS Base
CVSS3.1 Base
Bugtraq ID
Modified
Published
48242 Remote Management Service Accepting Unencrypted Credentials Detected (MSSQL) 3 Information gathering 7.5 7.3 07/29/2023 07/28/2023
106141 EOL/Obsolete Operating System: Microsoft Windows 10 Version 21H2 (HomeIProIPro EducationIPro for Workstations) Detected
Quick Actions
Info
Edit
curity 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
EOL/Obsolete Operating System: Microsoft Windows 10 Version 21H2 (HomeIProIPro EducationIPro for Workstations) Detected
Title: EOL/Obsolete Operating System: Microsoft Windows 10 Version 21H2 (HomeIProIPro EducationIPro 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: -

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.

Understanding the Vulnerability Knowledgebase

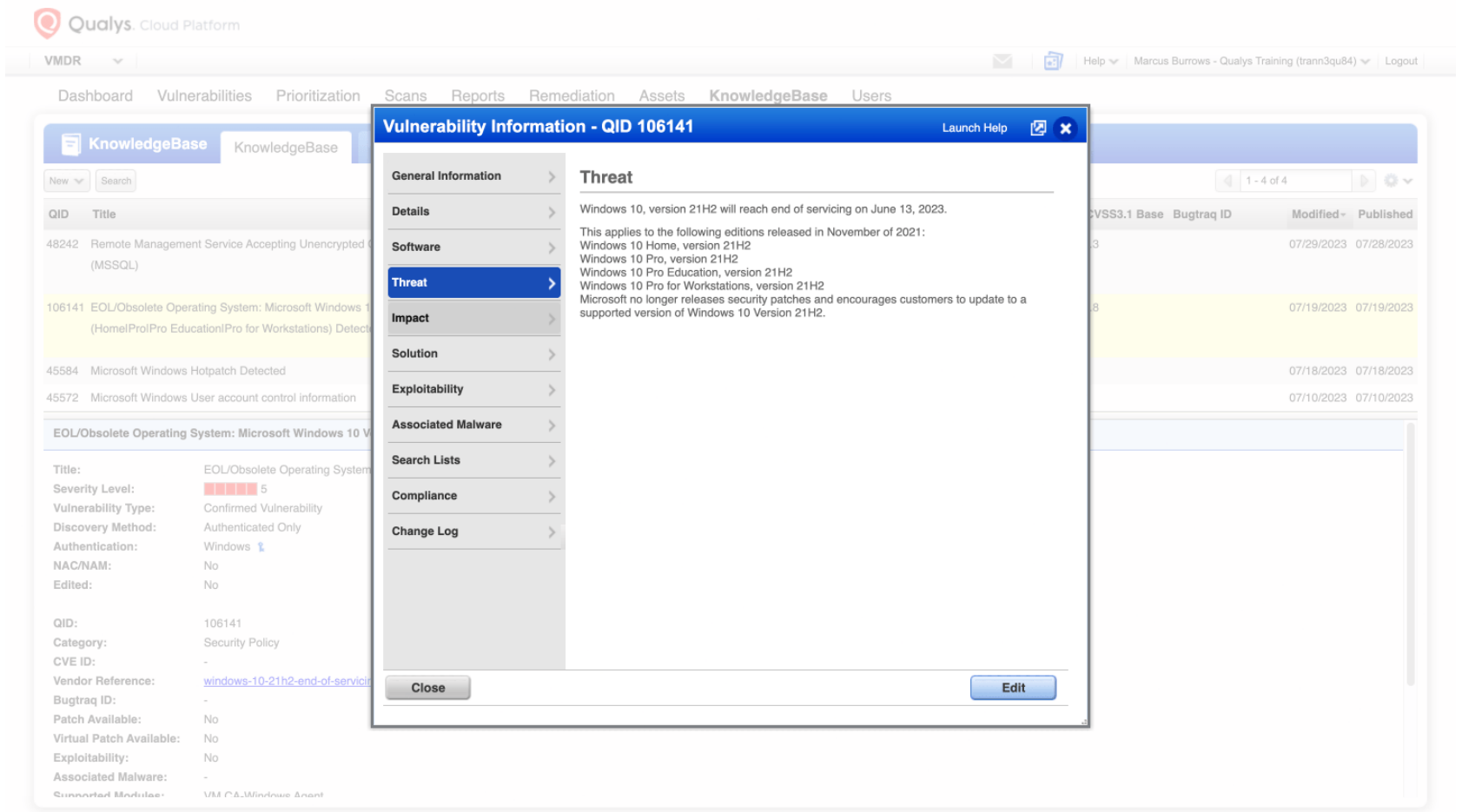


We can see again the vendor and product to which this vulnerability refers. Click on the Threat tab to continue.

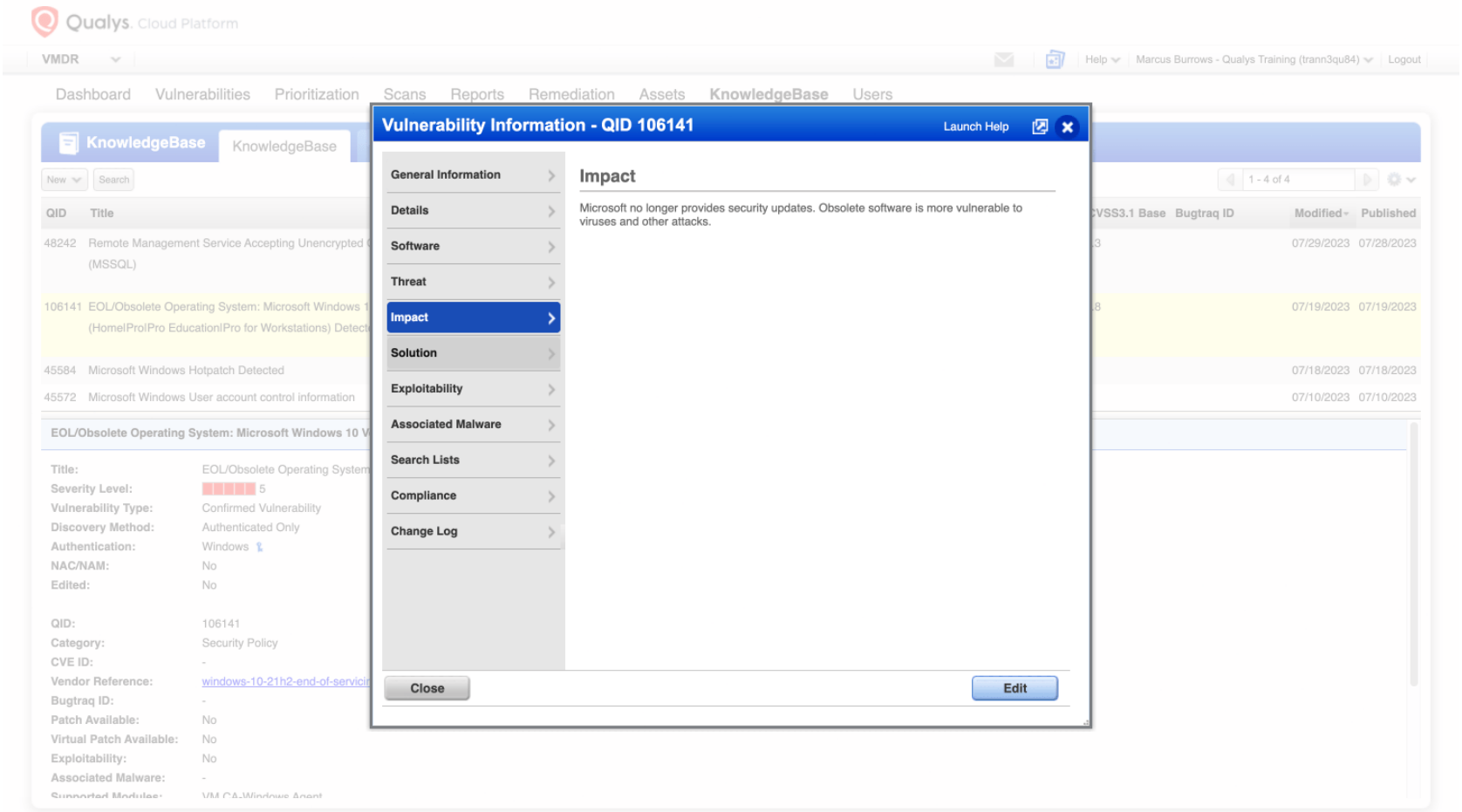


The Threat tab provides more details as to the nature of the threat and the specific editions of Windows which are affected. This could then be used to help guide our remediation strategy. Click on the Impact tab to continue.

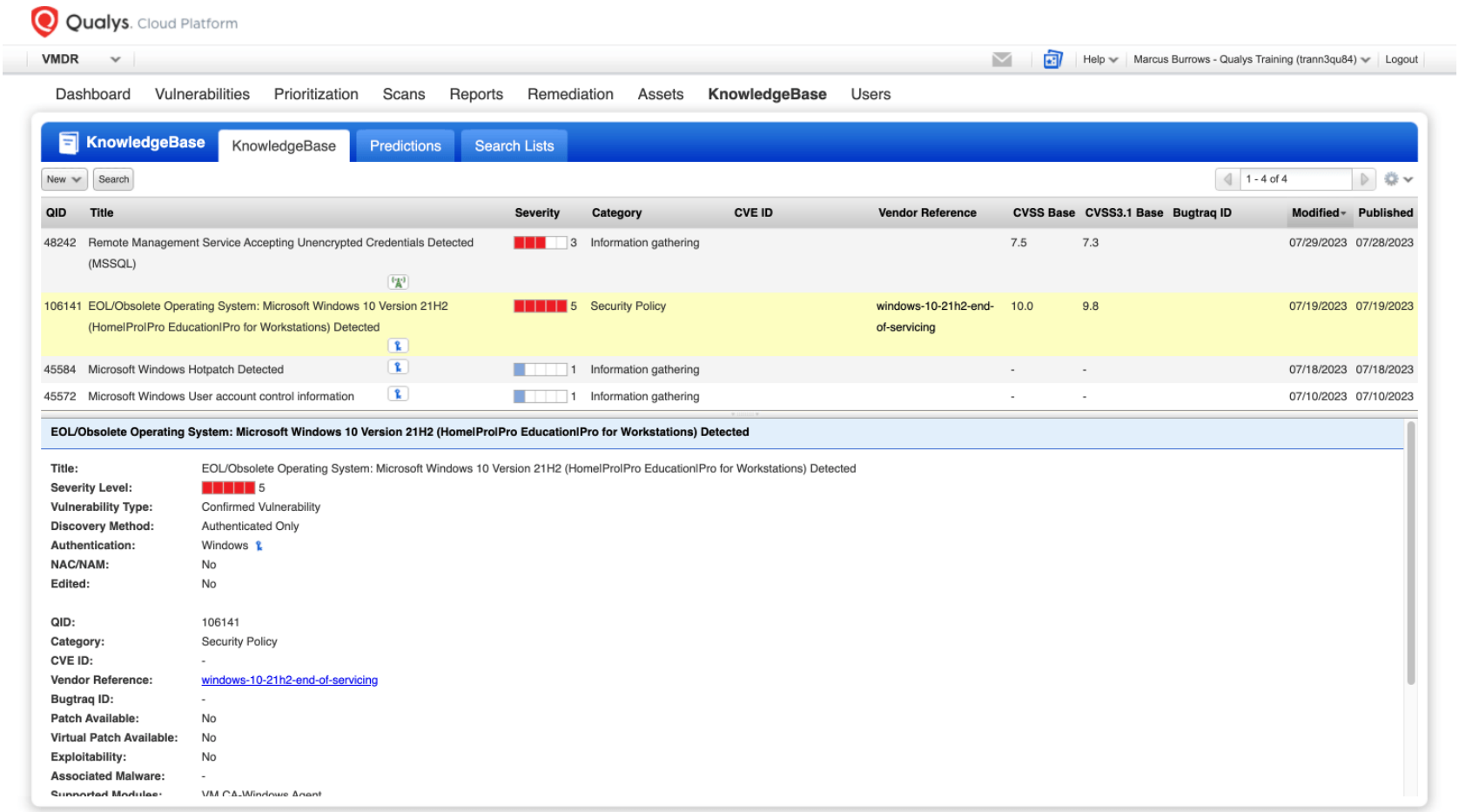
Understanding the Vulnerability Knowledgebase



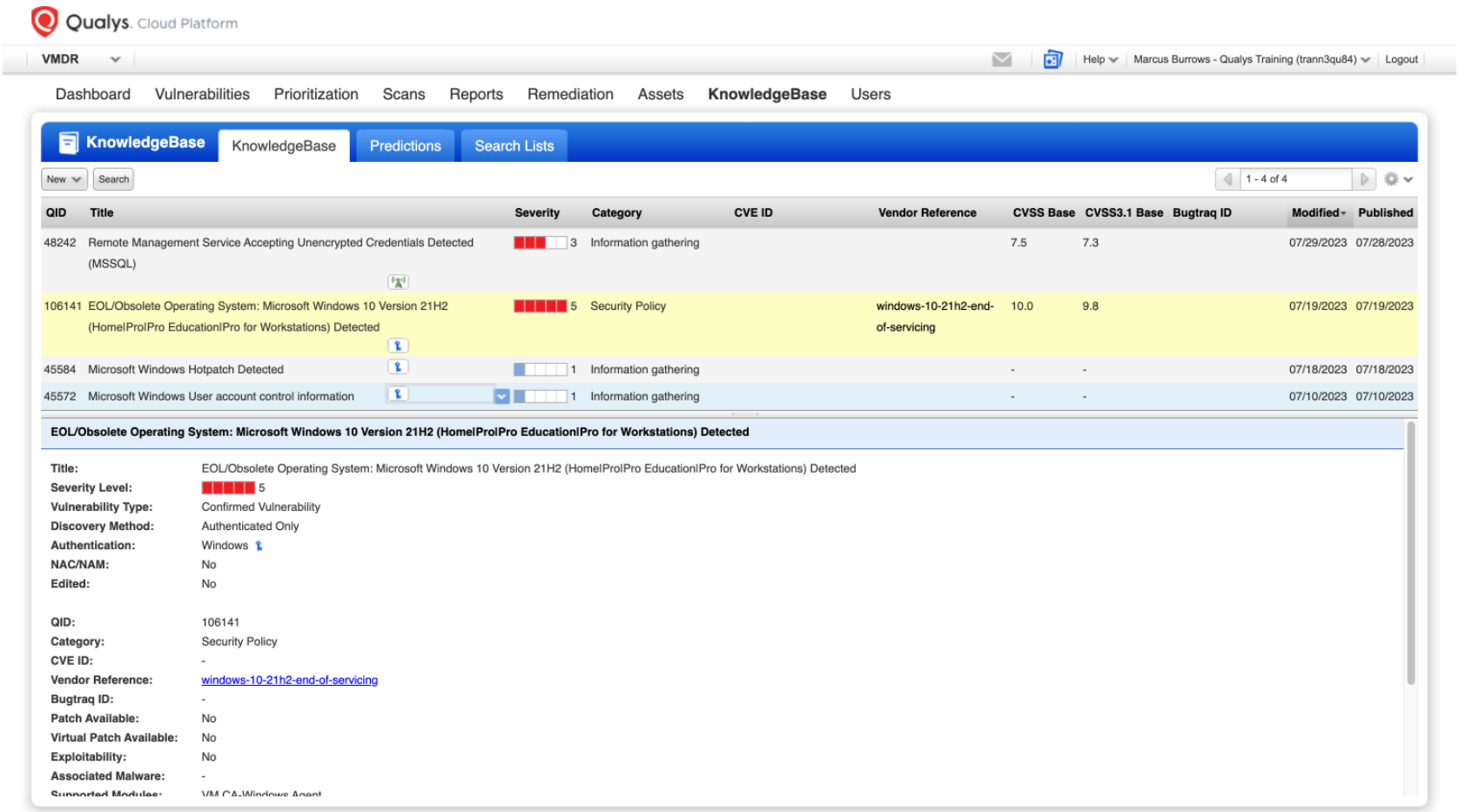
The Impact tab explains why the Severity Level is the highest. Click on the Close button to continue.



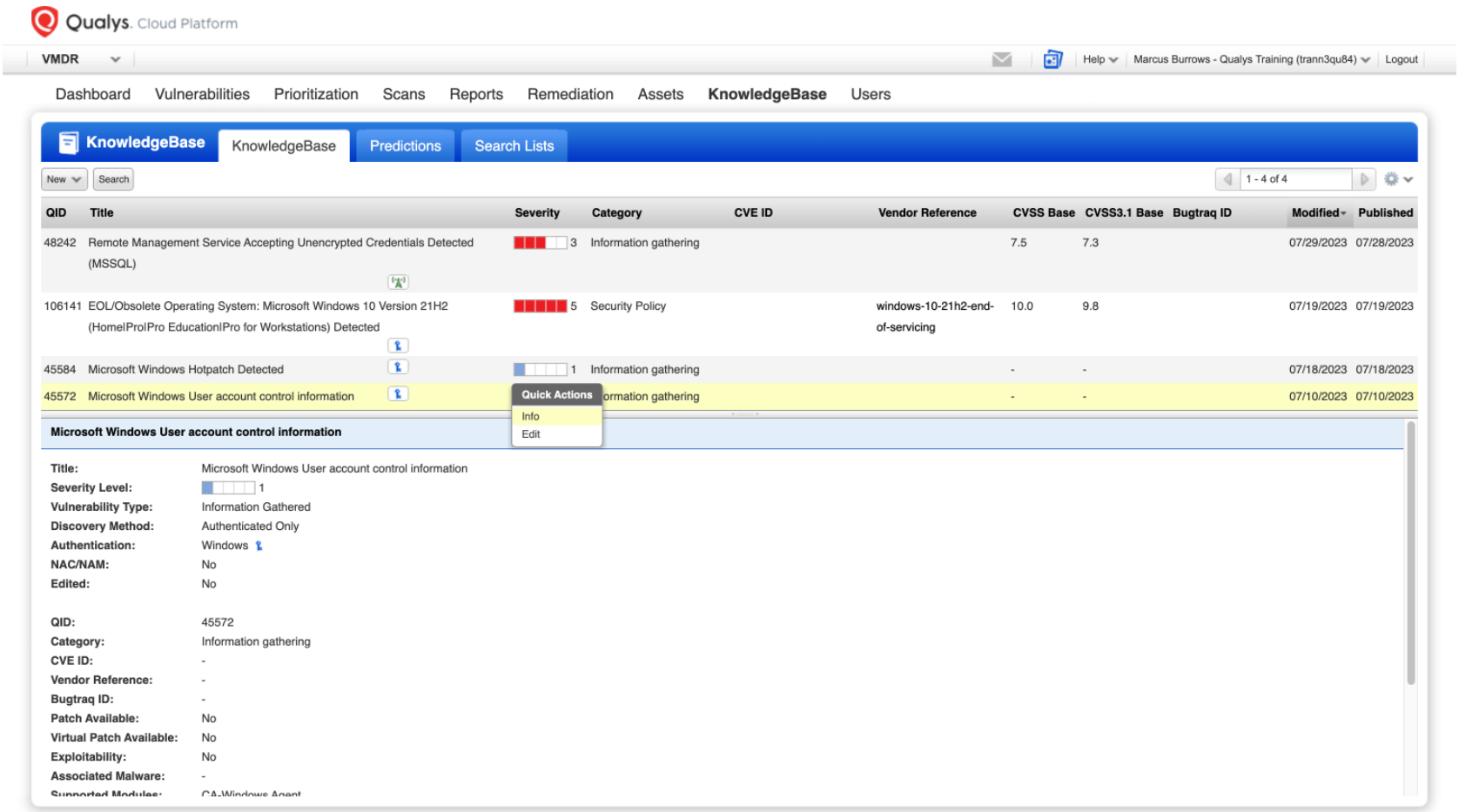
Now click on the last vulnerability in the list.



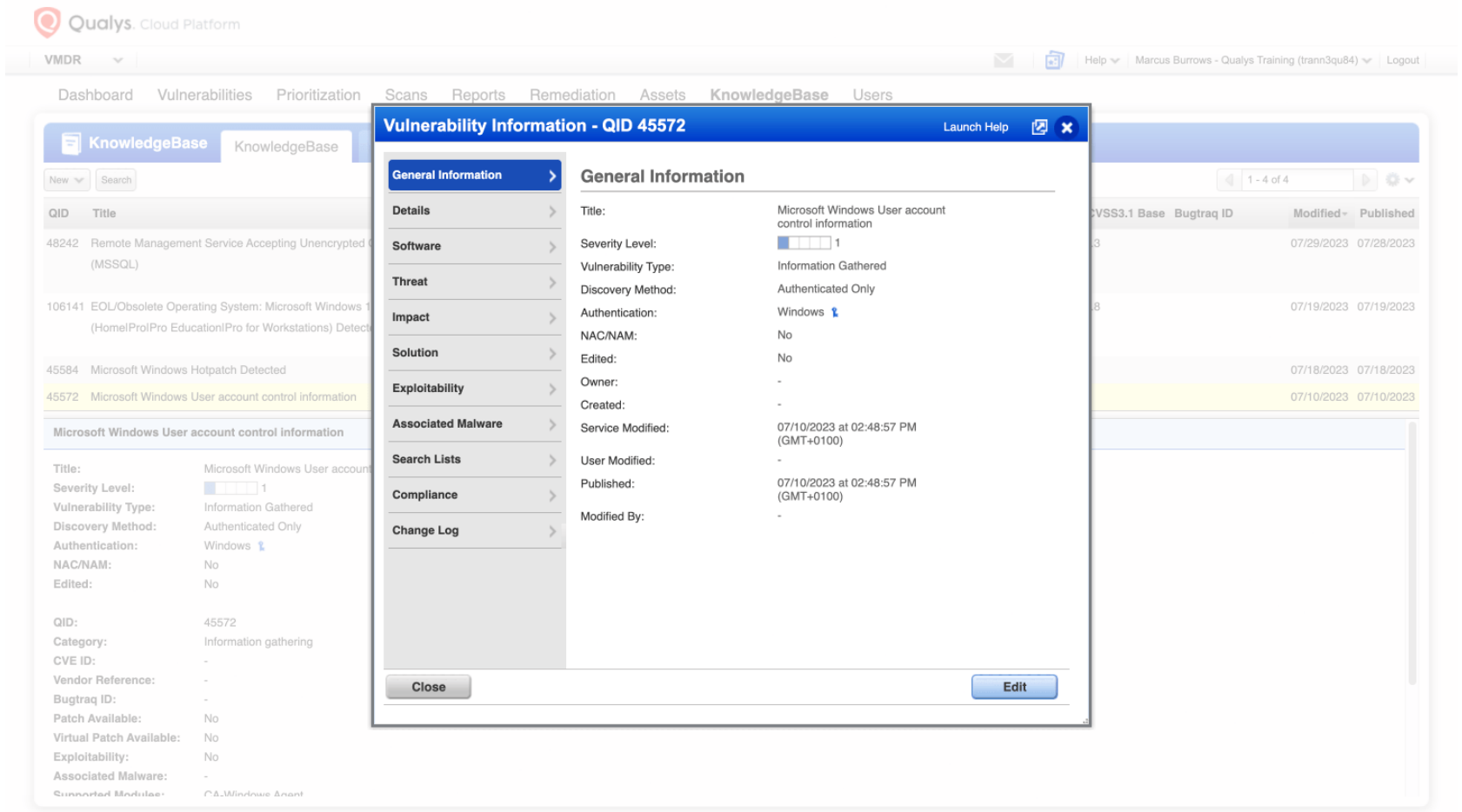
Click the drop down arrow.



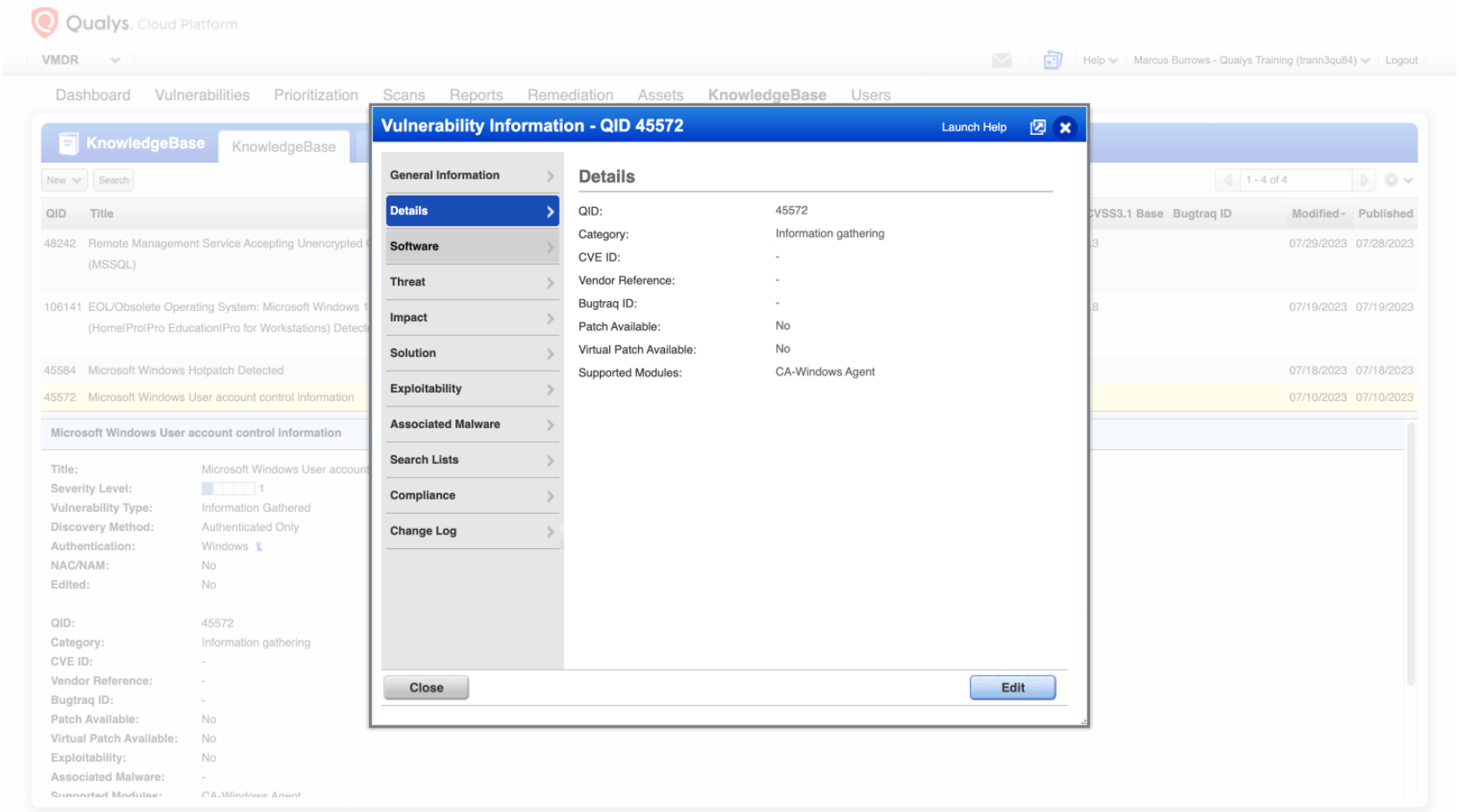
Click Info


Qualys. Cloud Platform
VMDR
Help
Marcus Burrows - Qualys Training (trann3qu84)
Logout
Dashboard
Vulnerabilities
Prioritization
Scans
Reports
Remediation
Assets
KnowledgeBase
Users
KnowledgeBase
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) 3 Information gathering 7.5 7.3 07/29/2023 07/28/2023
106141 EOL/Obsolete Operating System: Microsoft Windows 10 Version 21H2 (HomeIProIPro EducationIPro 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 ormation gathering - - 07/10/2023 07/10/2023
Quick Actions
Info
Edit
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: -

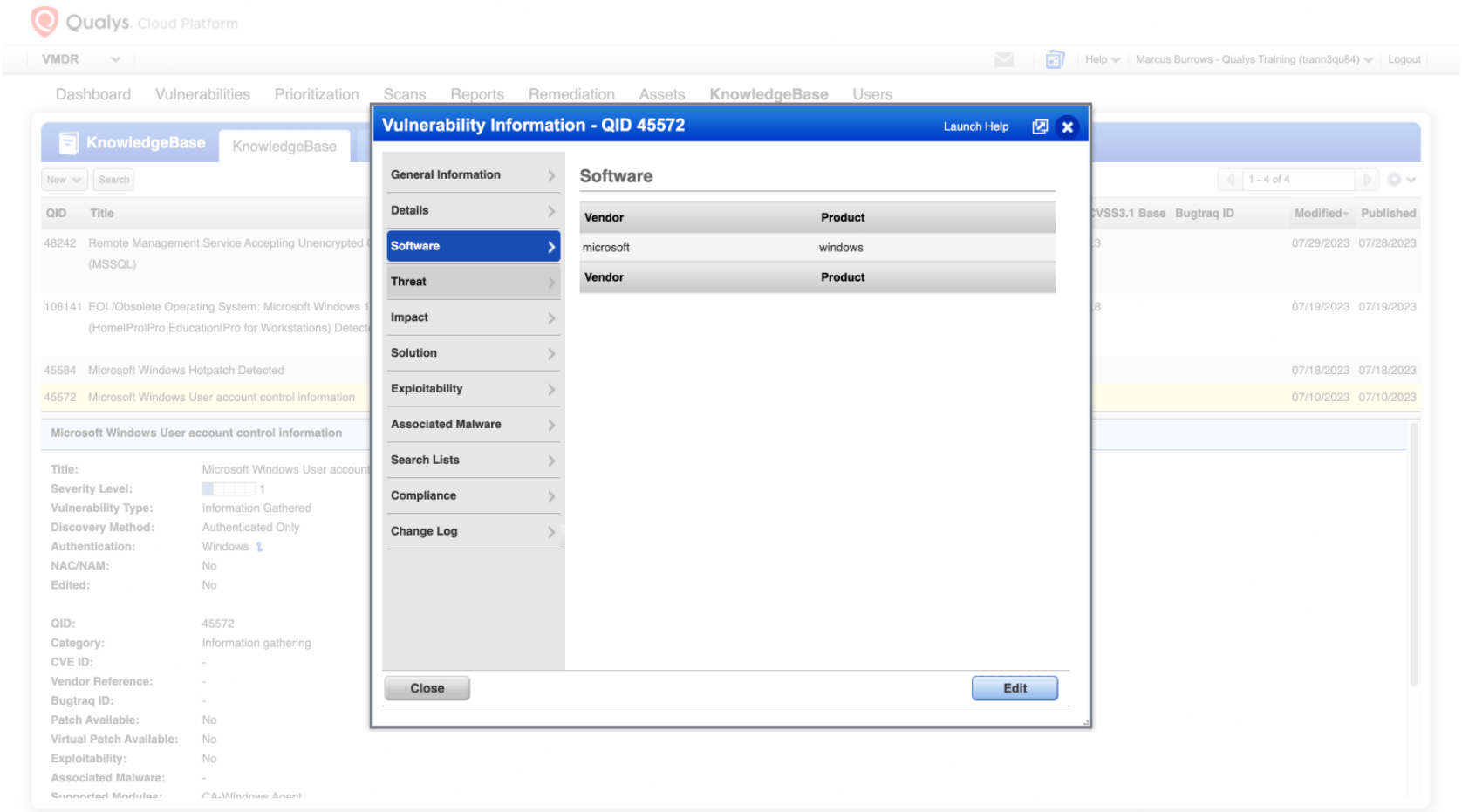
We can see that this Q.I.D. is not a vulnerability as such, but "Information Gathered". When included in the results of a scan, it will show user account control information. Click Details to continue.



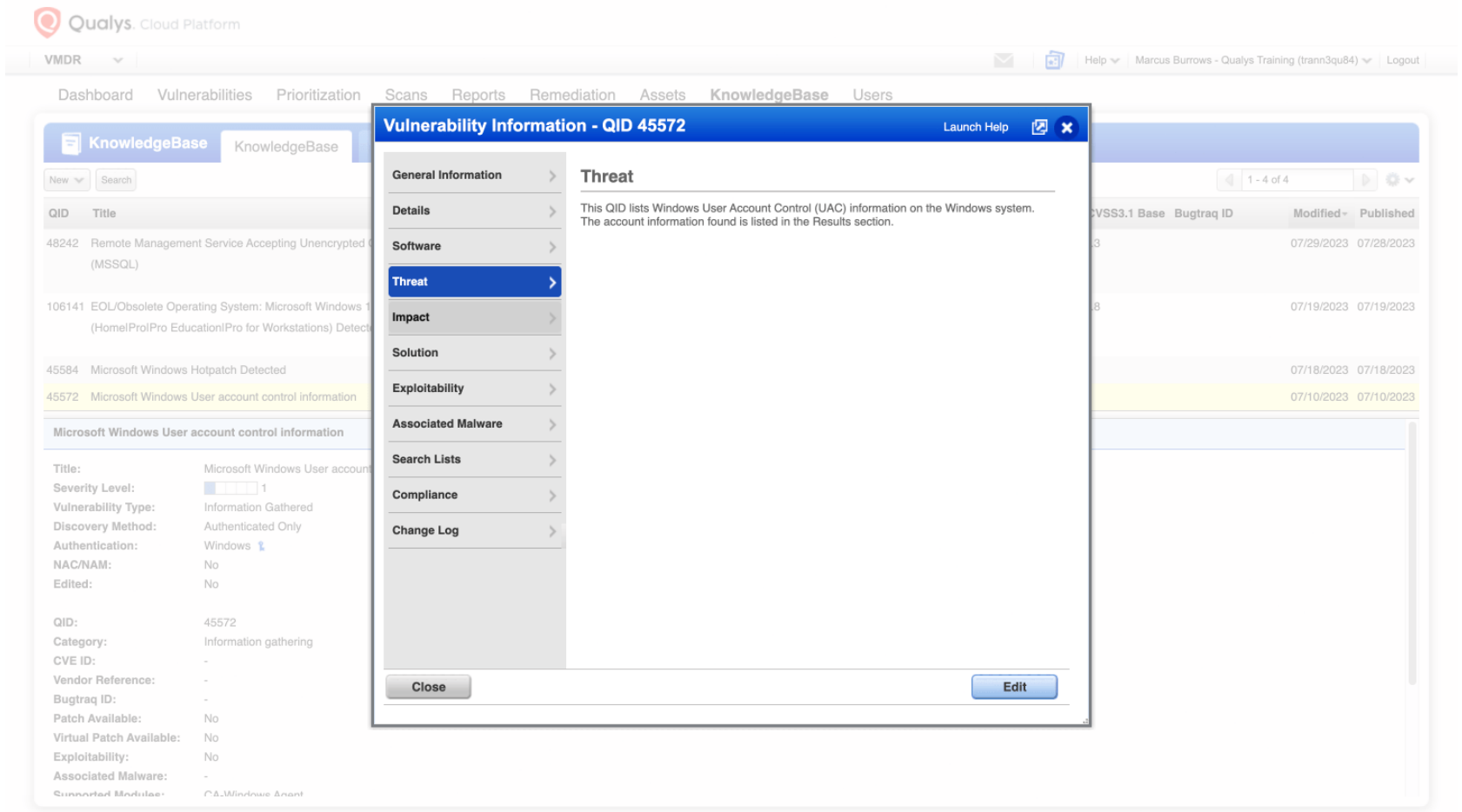
The Details tab, not surprisingly, does not show CVE or vendor references, as this is an Information Gathered Q.I.D. and not a discovered vulnerability. Click on the Software tab to continue.



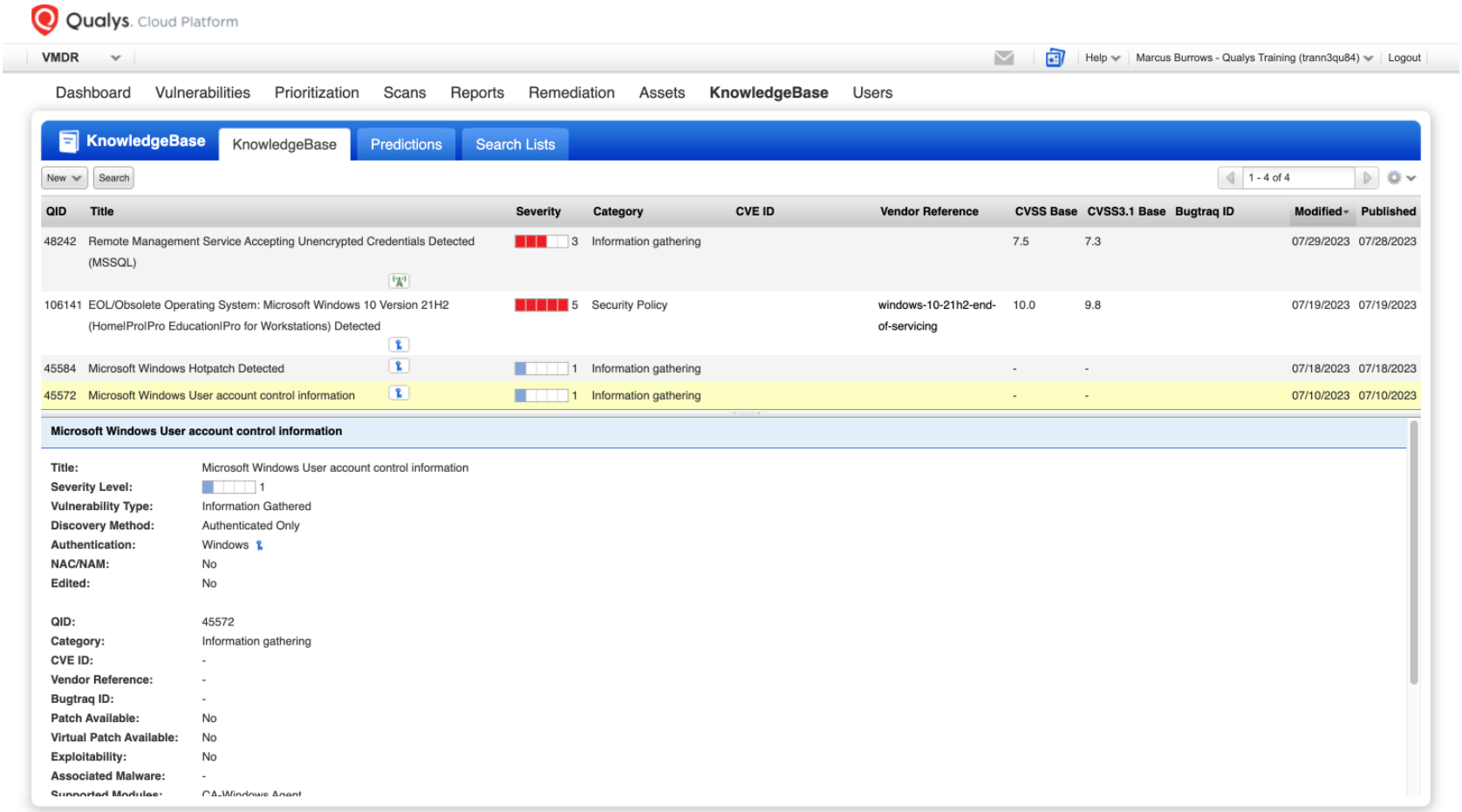
As before, the Software tab shows us the vendor and product. Click on the Threat tab to continue.



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.



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.



Scan to go to the interactive player