secpod

SanerNow

User Guide

Version 5.1

Vulnerability Management (VM)

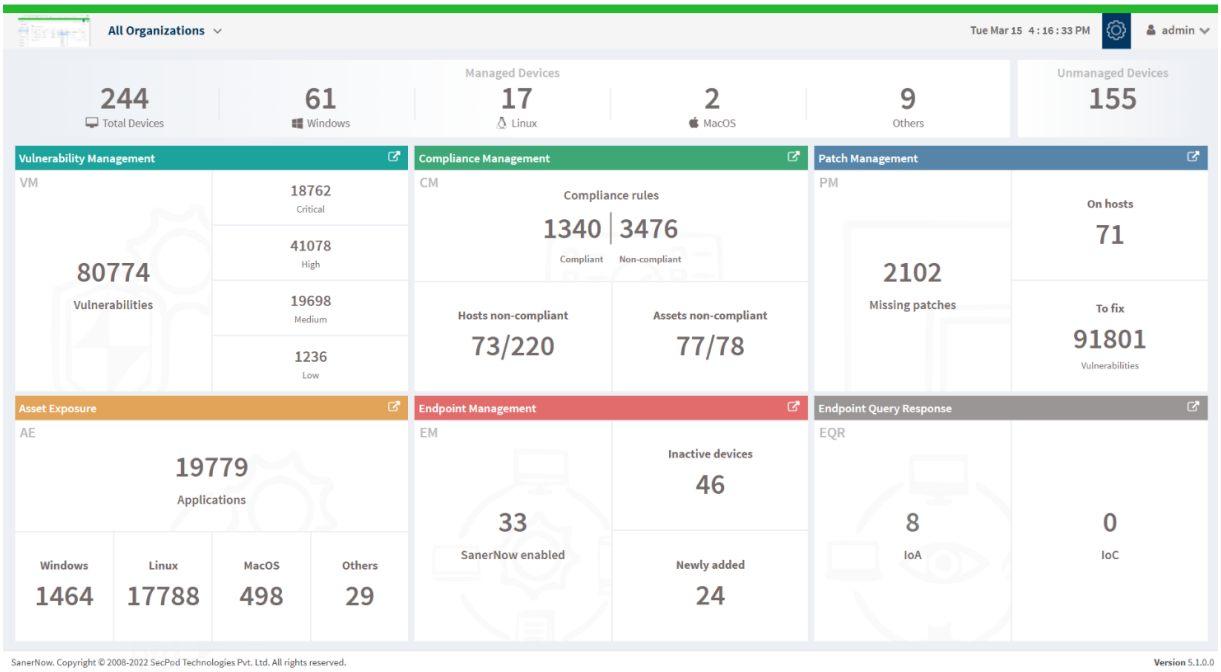
SanerNow provides a vulnerability management tool with impeccable vulnerability scans and instant remediation. Vulnerability management doesn't stop with scanning and detection; it comes with integrated patch management to remediate vulnerabilities instantly. SanerNow vulnerability management works as follows:

- **Scan and Identify:** It runs continuous scans and identifies vulnerabilities.
- **Assess and Prioritize:** Assess vulnerabilities and prioritize based on severity range.
- **Remediate and Report:** Remediate through patch management and report required actions.

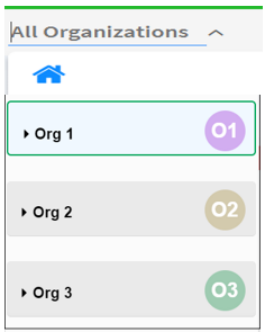
Monitor + Assess + Prioritize + Remediate = Vulnerability Management

SanerNow simplifies the vulnerability management cycle to a daily routine, simplifies remediation and reporting, and reduces the total cost of operation (TCO). The SanerNow solution helps identify, classify, remediate, and mitigate vulnerabilities in an organization. In the following sections, we will see how to accomplish Vulnerability Management with the SanerNow solution.

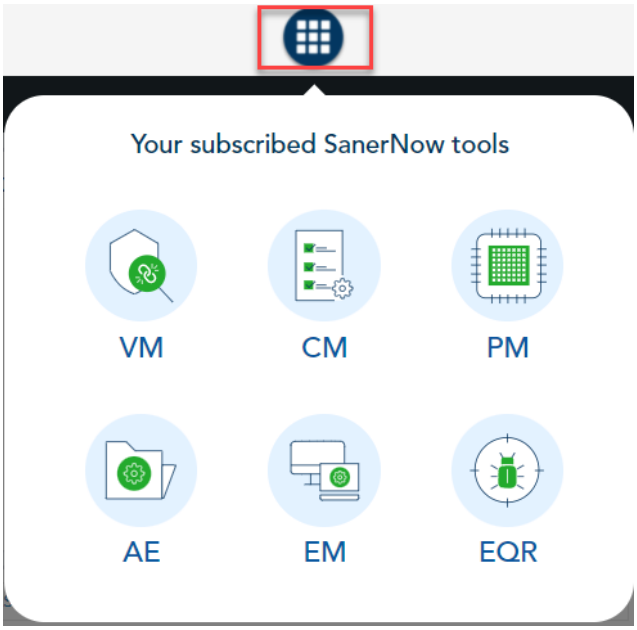
1. Log in to the SanerNow account with credentials.
2. Suppose an account already exists and the Saner Agent has been deployed on the endpoints; the organization level dashboard is displayed.



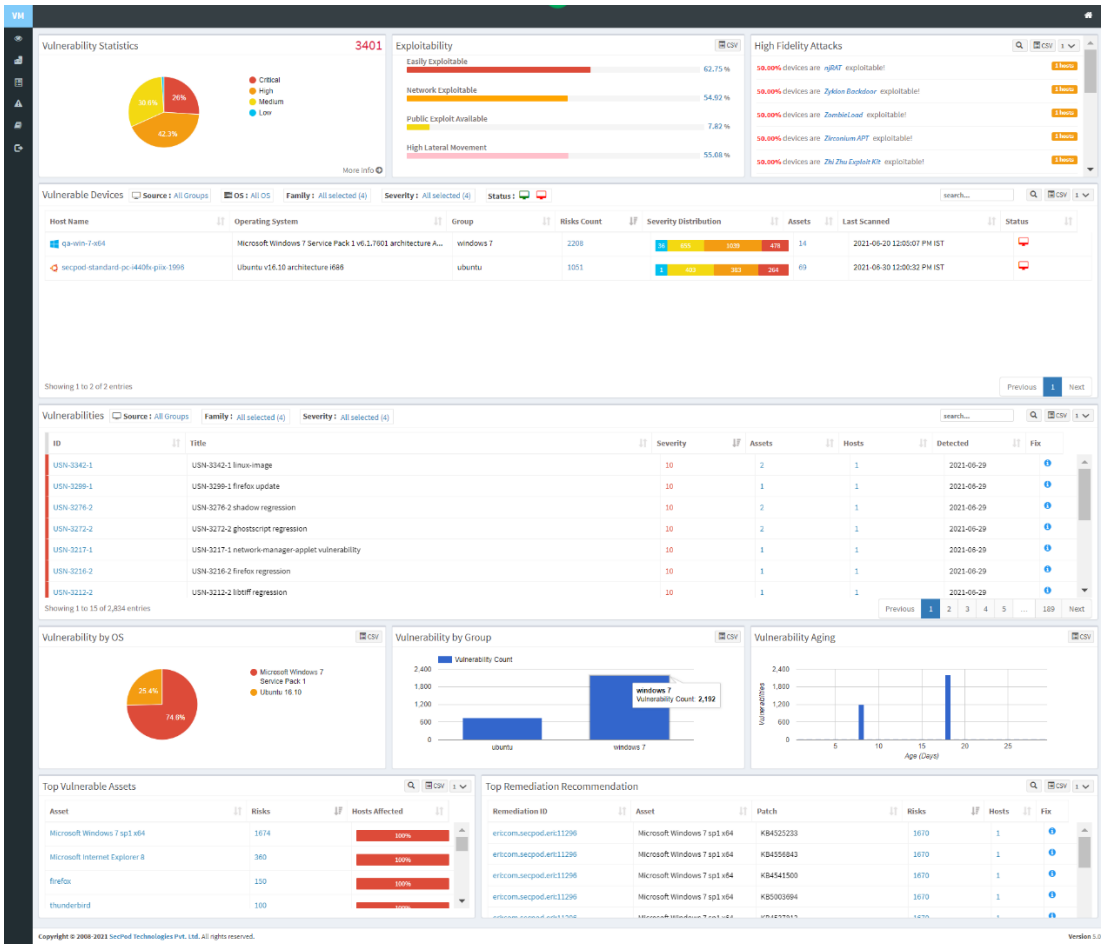
3. To select an account, click **All Organizations** on the top left corner of the dashboard. All Organization section lists all the organizations. You can see the list of organizations as Org1, Org2, and Org3, as shown below; select the account, and a dashboard with the summary view of the account is displayed.



4. Click the SanerNow tools icon on the header. It will display all the provision tools, as shown below.



5. Click on the Vulnerability Management icon. The Vulnerability Dashboard is displayed, which provides vulnerability details categorized by severity or type, age, affected hosts, vulnerable devices, and vulnerabilities.

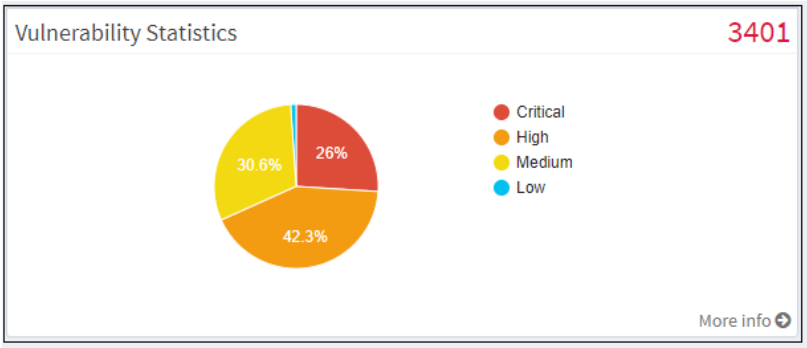


SanerNow hosts the world's largest vulnerability database with around 100,000+ security checks. The latest vulnerability checks are constantly fed to the SCAP repository. SanerNow thoroughly analyses these vulnerabilities and prioritizes them based on their severity. Easily manage and control all vulnerability management tasks from an all-in-one centralized console. Gain insights on various vulnerability

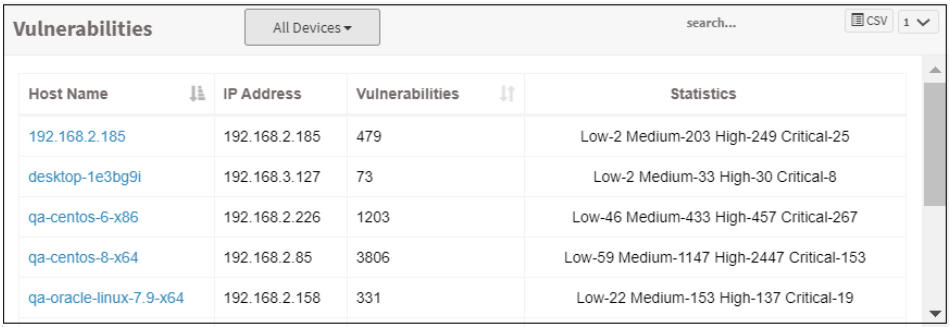
management attribute from the centralized dashboard. View the exploit potential of the detected vulnerabilities evaluated based on the CVSS score.

Vulnerability Statistics

It is important to prioritize the vulnerabilities based on the severity levels and plan the remediation. SecPod uses the Common Vulnerability Scoring System (CVSS), which determines the severity of the vulnerability based on principal characteristics. The Vulnerability Statistics pane shows the total number of vulnerabilities in the network and classifies the severity of the vulnerabilities as low, medium, high, and critical.



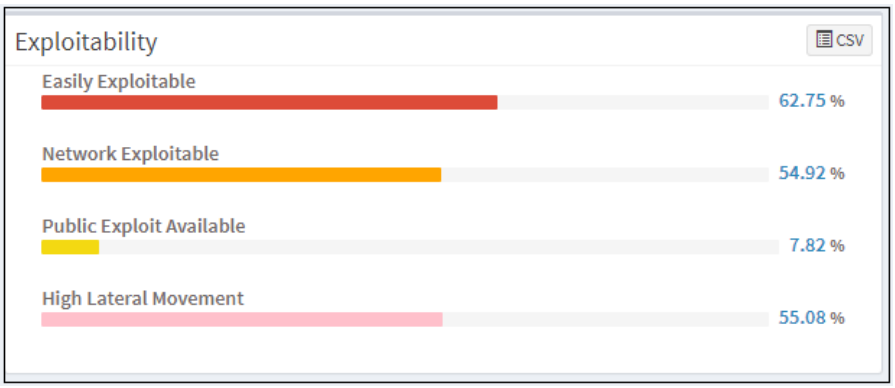
Click on the **More Info** link, which shows a dialog box to filter the vulnerability statistics by all devices, unassigned devices, groups, or a specific group of devices. The affected device or hostname, the IP address, the total number of vulnerabilities for that host, and the severity grouping is displayed in the dialog.



Host Name	IP Address	Vulnerabilities	Statistics
192.168.2.185	192.168.2.185	479	Low-2 Medium-203 High-249 Critical-25
desktop-1e3bg9i	192.168.3.127	73	Low-2 Medium-33 High-30 Critical-8
qa-centos-6-x86	192.168.2.226	1203	Low-46 Medium-433 High-457 Critical-267
qa-centos-8-x64	192.168.2.85	3806	Low-59 Medium-1147 High-2447 Critical-153
qa-oracle-linux-7.9-x64	192.168.2.158	331	Low-22 Medium-153 High-137 Critical-19

Exploitability

Remediation can be prioritized if there is visibility into the vulnerability category. You can download the excel sheet by clicking on the CSV icon. The file contains information about the vulnerabilities based on the exploitability.

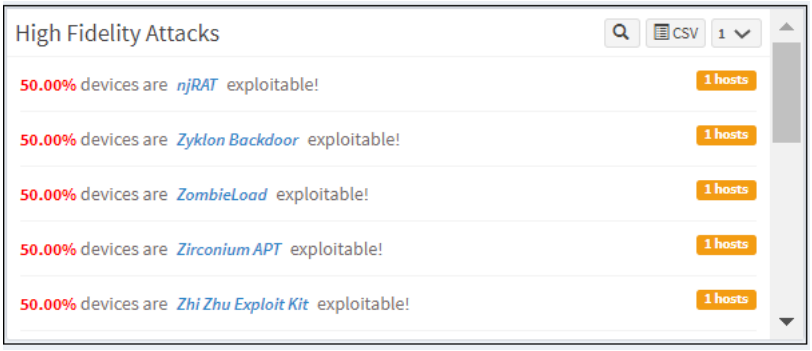


This page categorizes the vulnerabilities on the network by:

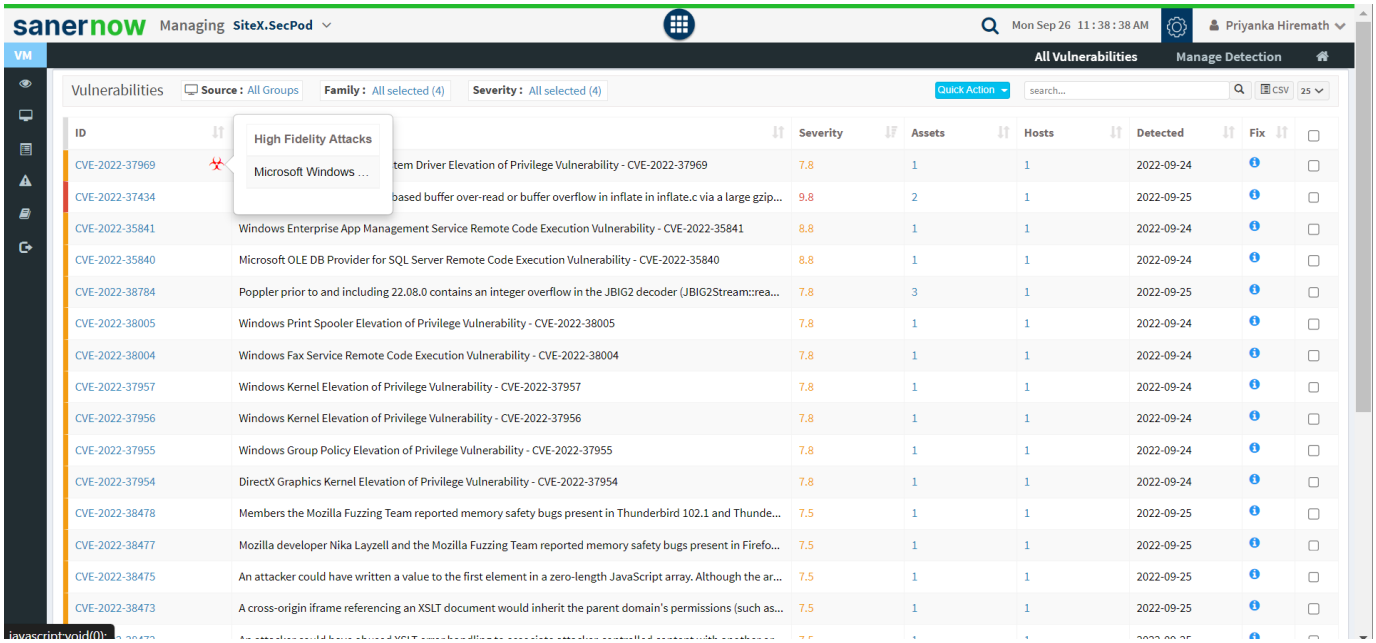
- **Easily Exploitable:** Vulnerabilities are known in the public domain, making an exploit easily possible.
- **Network Exploitable:** Vulnerabilities can be exploited with remote network access. The attacker's path is through the network layer.
- **Public Exploit Available:** Vulnerabilities for which publicly available exploits have occurred in the past.
- **High Lateral Movement:** Vulnerabilities extend to the network as the threat moves from device to device and asset to asset, and attackers collect valuable data.

High Fidelity Attacks

High fidelity attacks pane groups, the vulnerabilities by the exploit kits that can be used to exploit the weakness. This pane shows the high-fidelity attacks which defect the array of attacks vulnerability leads to. In this way, SanerNow predicts having the vulnerability in an organization. On clicking on the highlighted attack name, you will get a description model of the attack. You can download the excel sheet with detailed information by clicking on the CSV icon.



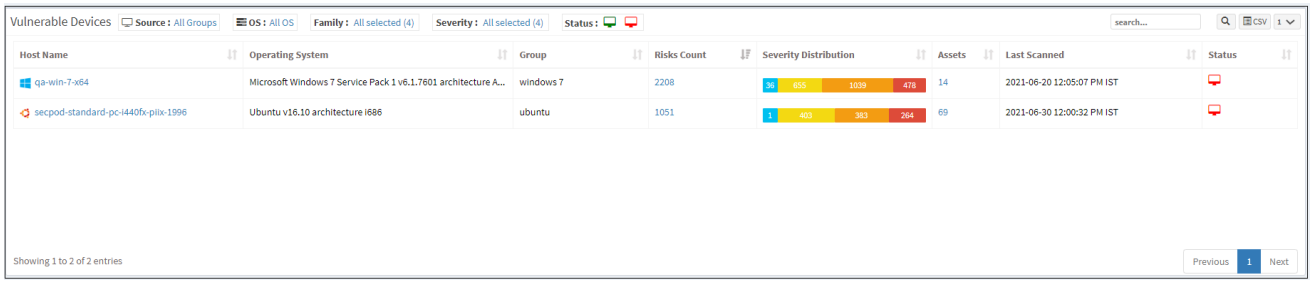
SanerNow is introduced with a new icon for high-fidelity attacks. You can view the individual vulnerabilities associated with high-profile attacks in the All Vulnerabilities dashboard. You can act on these critical vulnerabilities by remediating or excluding them through the Quick Action section.



Vulnerable Devices

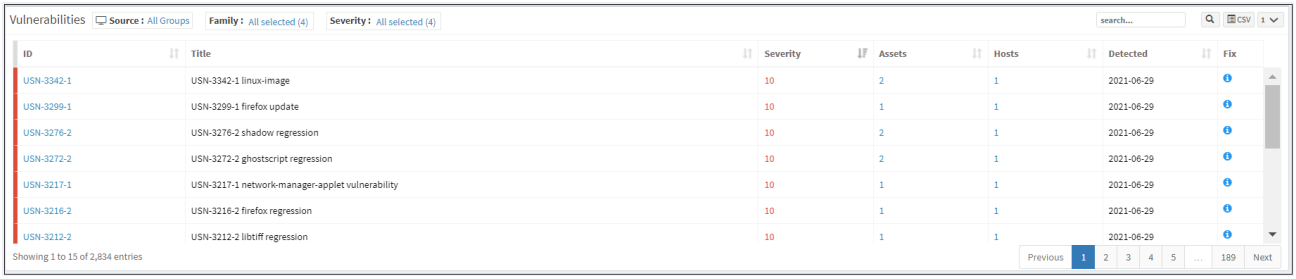
This pane lists vulnerable devices with detailed information on risk count based on severity distribution. This pane displays all the devices in the network along with the hostname, operating system, group, count,

severity distribution, assets count, last scanned information, and device status. Filter options are provided to narrow the search based on the groups, operating system, family, and status. The Others option in the Family filter will list the network devices. You can download the excel sheet with vulnerable device information by clicking on the CSV icon.



Vulnerabilities

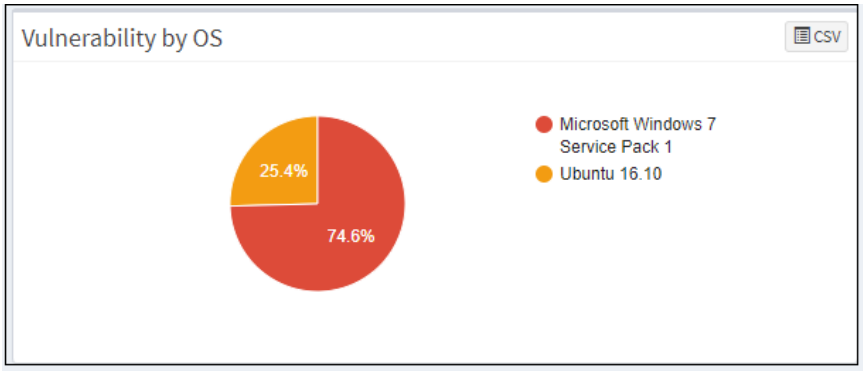
This page lists the vulnerabilities with detailed information. You can see the CVE ID of the vulnerabilities, vulnerable title, detected time, and how many hosts it affected. Filters are provided to filter the vulnerabilities based on group, family, and severity. You can download the excel sheet with vulnerabilities information by clicking on the CSV icon.



You will get fixed information by moving a cursor on the (i) icon. To get more details about the vulnerabilities, click on the CVE id, which redirects to the SCAP repository page. This page will display complete information about the vulnerability and CVSS score. The severity level is calculated based on the CVSS score.

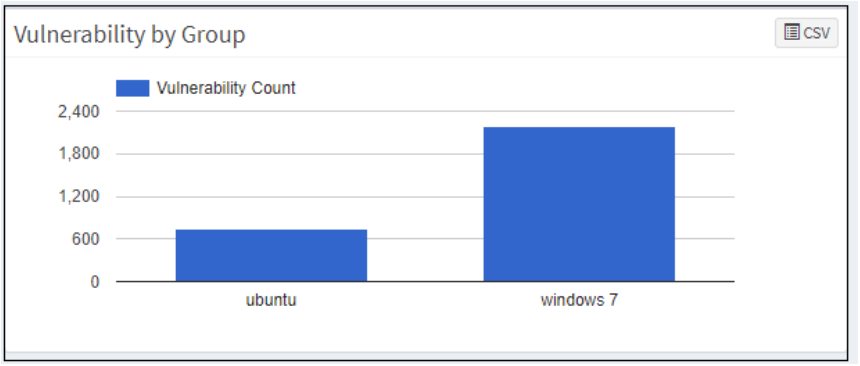
Vulnerability by OS

This page shows the list of vulnerabilities categorized by the operating system with the help of a pie chart. You can download the excel sheet with the list of vulnerabilities based on the operating system by clicking on the CSV icon.



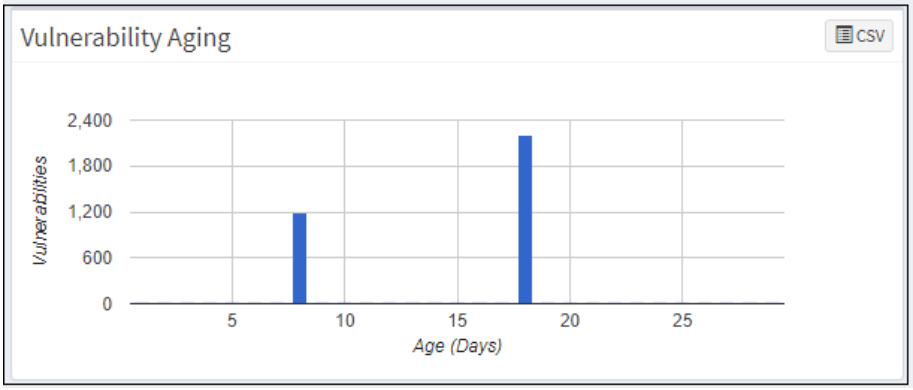
Vulnerability by Group

This page shows the list of vulnerabilities, categorized by the groups with the help of a graph. You can download the excel sheet with a list of vulnerabilities based on the group by clicking on the CSV icon.



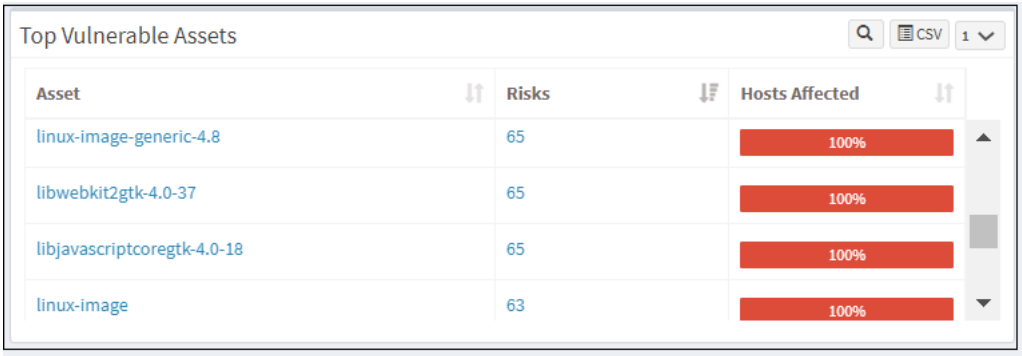
Vulnerability Aging

This pane shows vulnerabilities grouped by aging. The number of days since they were detected has not been fixed. The pane shows the age of each vulnerability in an account after its detection. You can download the excel sheet with a list of vulnerabilities based on age by clicking on the CSV icon.



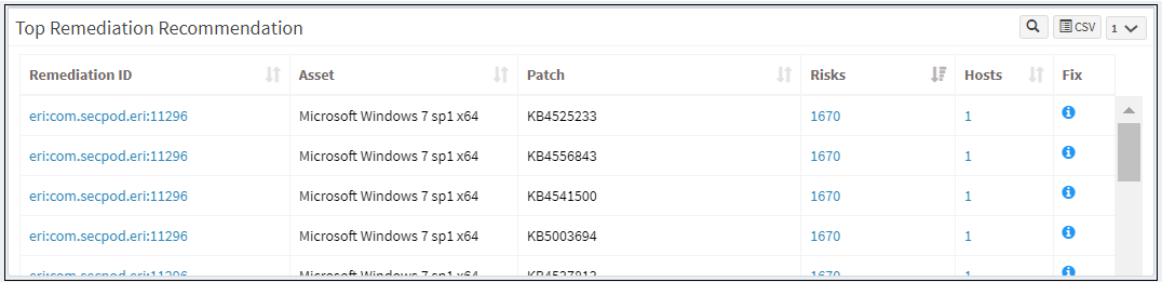
Top Vulnerable Assets

This pane shows the top vulnerable assets by their CVE ID and the number of devices at risk. You can download the excel sheet with the asset information by clicking on the CSV icon. The search option is provided to search the asset with the asset name.



Top Remediation Recommendation

This page lists the top remediation recommended based on the CRE. It will list remediations that can address a maximum number of deviations. You can download the CSV file by clicking on the CSV icon.



Remediation ID	Asset	Patch	Risks	Hosts	Fix
eri:com.secpod.eri:11296	Microsoft Windows 7 sp1 x64	KB4525233	1670	1	
eri:com.secpod.eri:11296	Microsoft Windows 7 sp1 x64	KB4556843	1670	1	
eri:com.secpod.eri:11296	Microsoft Windows 7 sp1 x64	KB4541500	1670	1	
eri:com.secpod.eri:11296	Microsoft Windows 7 sp1 x64	KB5003694	1670	1	

All Vulnerabilities Dashboard

SanerNow introduces a new dashboard where you can view all the vulnerabilities with CVE IDs, severity, the number of assets affected, detected dates, and fix information. You are also provided with a search bar where you can search for exploit-specific keywords. You can act on these vulnerabilities by excluding them or by remediating them through the Quick Action section.

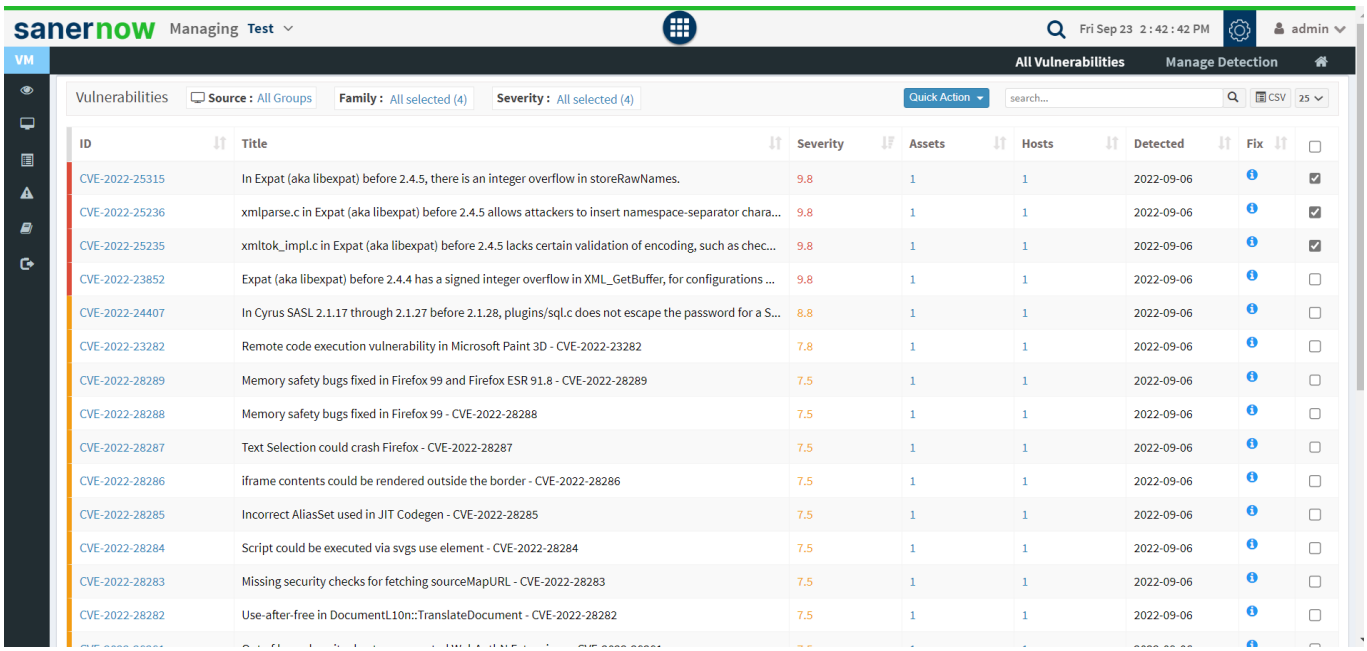
Exclude Vulnerabilities

SanerNow facilitates dealing with false positives and vulnerabilities that do not apply to their environment. You can exclude and view them using the vulnerability management module.

There are three ways to exclude vulnerabilities:

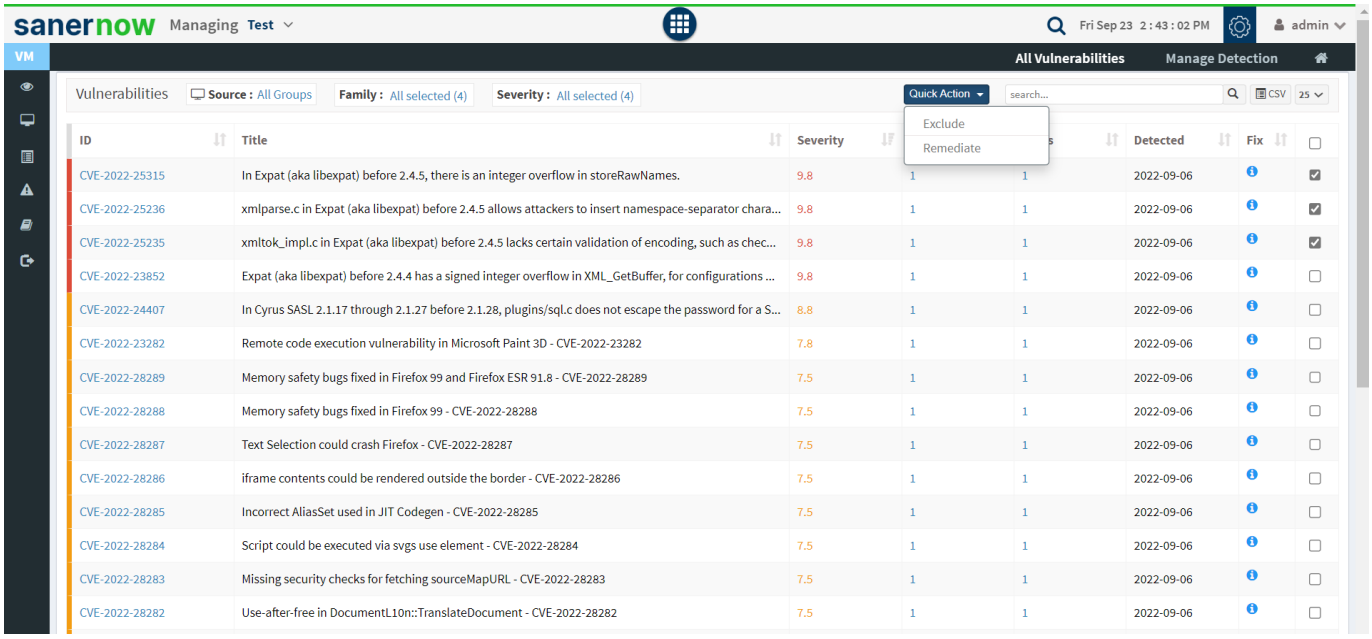
1. **From All vulnerability dashboard**

- In All Vulnerabilities, you will have the vulnerability details like CVE ID, Title, Severity, Date of detection, Host, and Information of Fix. Select the vulnerability from the check box that is to be excluded.

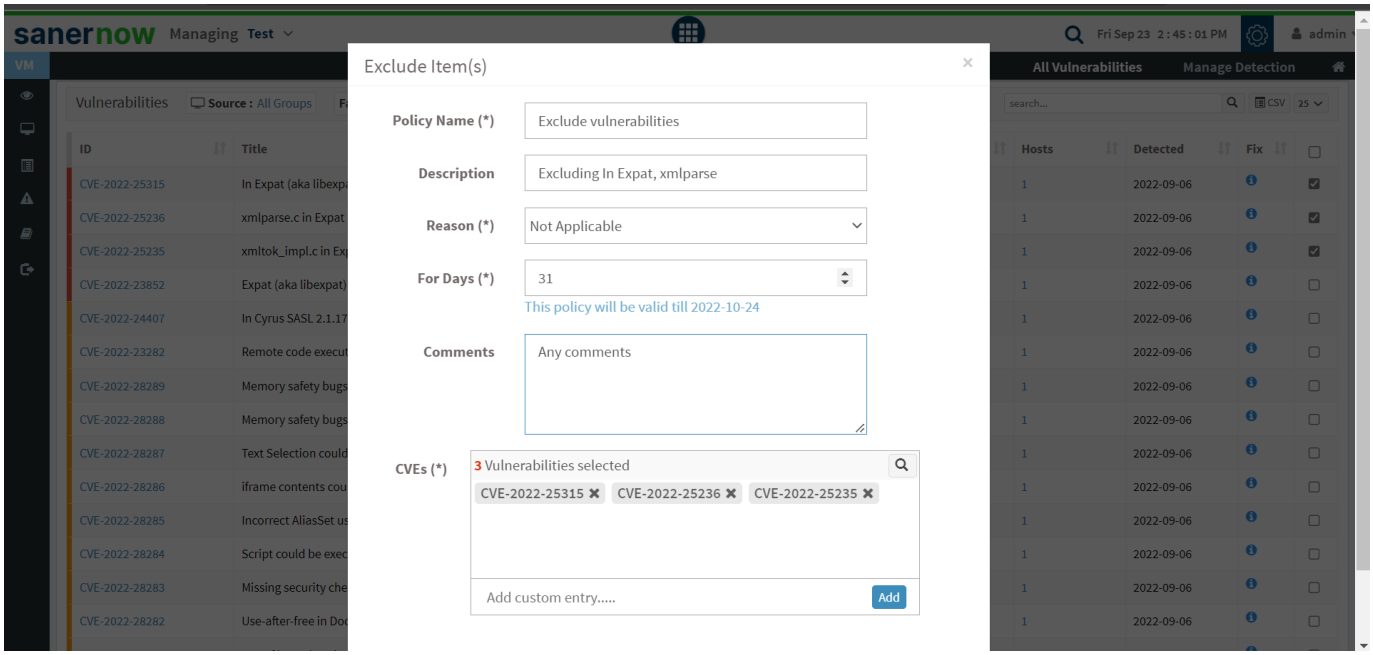


ID	Title	Severity	Assets	Hosts	Detected	Fix
CVE-2022-25315	In Expat (aka libexpat) before 2.4.5, there is an integer overflow in storeRawNames.	9.8	1	1	2022-09-06	
CVE-2022-25236	xmlparse.c in Expat (aka libexpat) before 2.4.5 allows attackers to insert namespace-separator chara...	9.8	1	1	2022-09-06	
CVE-2022-25235	xmltok_impl.c in Expat (aka libexpat) before 2.4.5 lacks certain validation of encoding, such as chec...	9.8	1	1	2022-09-06	
CVE-2022-23852	Expat (aka libexpat) before 2.4.4 has a signed integer overflow in XML_GetBuffer, for configurations ...	9.8	1	1	2022-09-06	
CVE-2022-24407	In Cyrus SASL 2.1.17 through 2.1.27 before 2.1.28, plugins/sql.c does not escape the password for a S...	8.8	1	1	2022-09-06	
CVE-2022-23282	Remote code execution vulnerability in Microsoft Paint 3D - CVE-2022-23282	7.8	1	1	2022-09-06	
CVE-2022-28289	Memory safety bugs fixed in Firefox 99 and Firefox ESR 91.8 - CVE-2022-28289	7.5	1	1	2022-09-06	
CVE-2022-28288	Memory safety bugs fixed in Firefox 99 - CVE-2022-28288	7.5	1	1	2022-09-06	
CVE-2022-28287	Text Selection could crash Firefox - CVE-2022-28287	7.5	1	1	2022-09-06	
CVE-2022-28286	iframe contents could be rendered outside the border - CVE-2022-28286	7.5	1	1	2022-09-06	
CVE-2022-28285	Incorrect AliasSet used in JIT Codegen - CVE-2022-28285	7.5	1	1	2022-09-06	
CVE-2022-28284	Script could be executed via svgs use element - CVE-2022-28284	7.5	1	1	2022-09-06	
CVE-2022-28283	Missing security checks for fetching sourceMapURL - CVE-2022-28283	7.5	1	1	2022-09-06	
CVE-2022-28282	Use-after-free in DocumentL10n::TranslateDocument - CVE-2022-28282	7.5	1	1	2022-09-06	

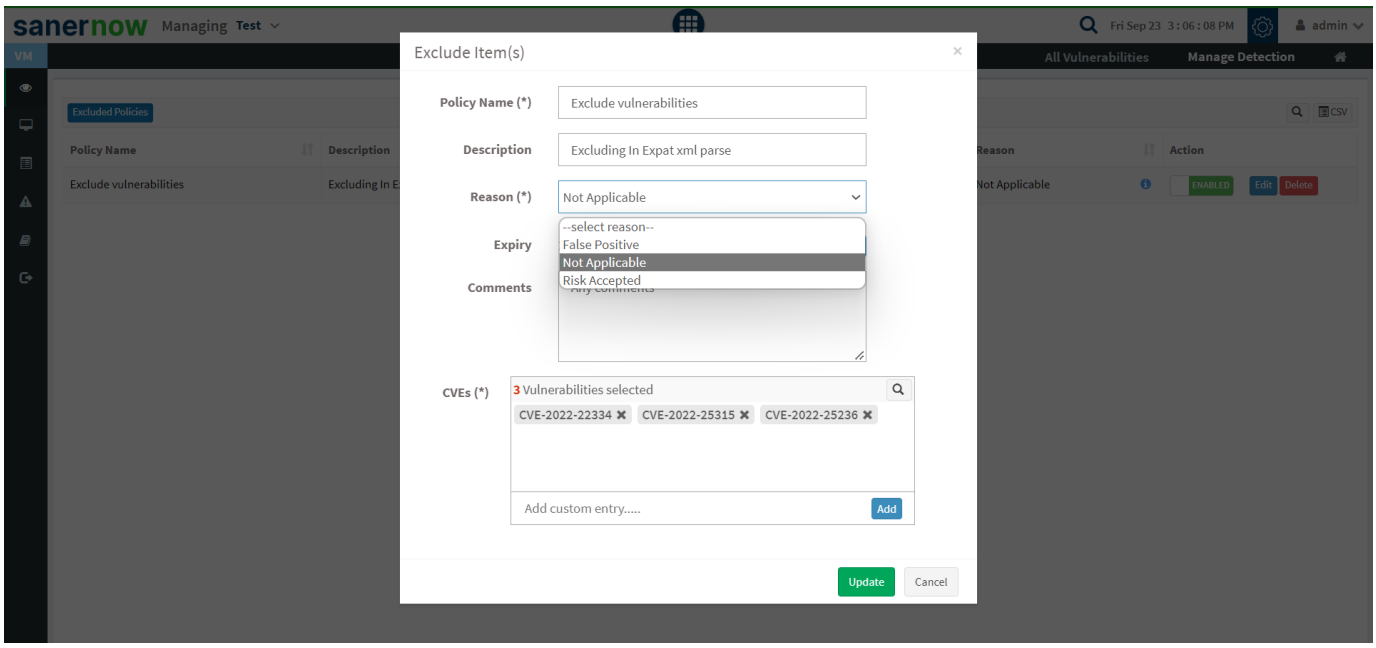
- Click on Quick Action. You can exclude or remediate. For remediation, you will be redirected to the Patch Management module. (Given that you subscribed to the patch management module)



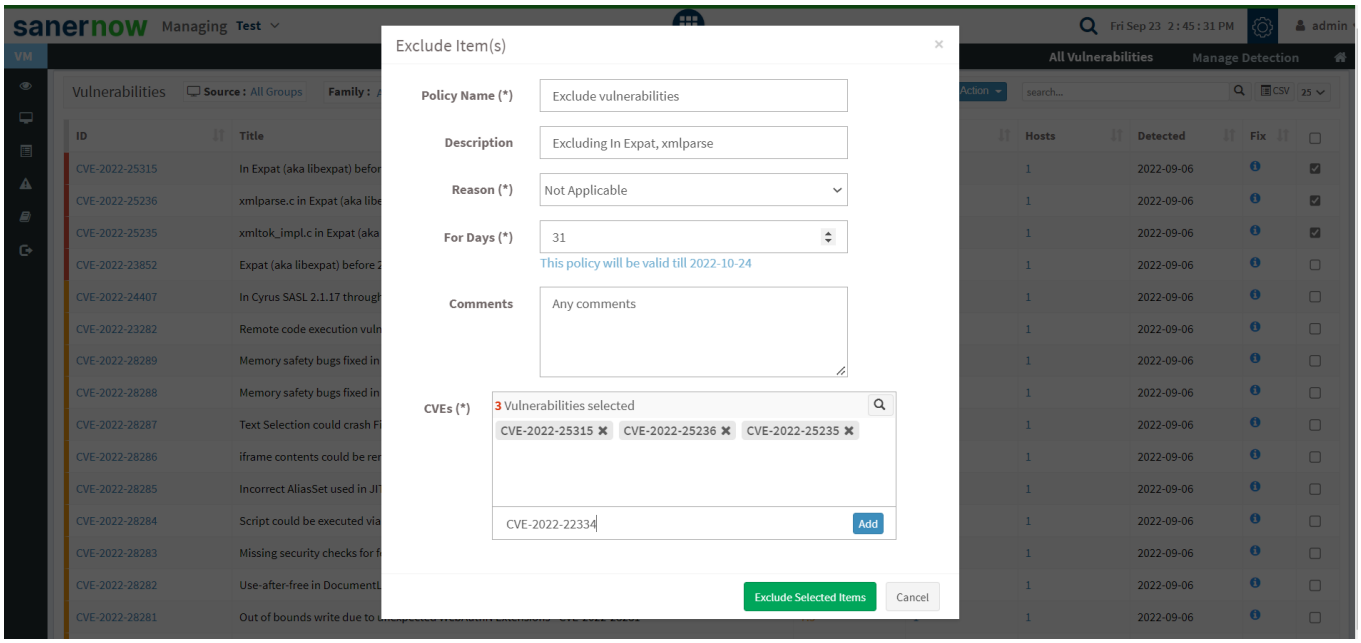
- Select Exclude and fill up all the vulnerability exclude details.
- Give Policy Name and Policy Description.

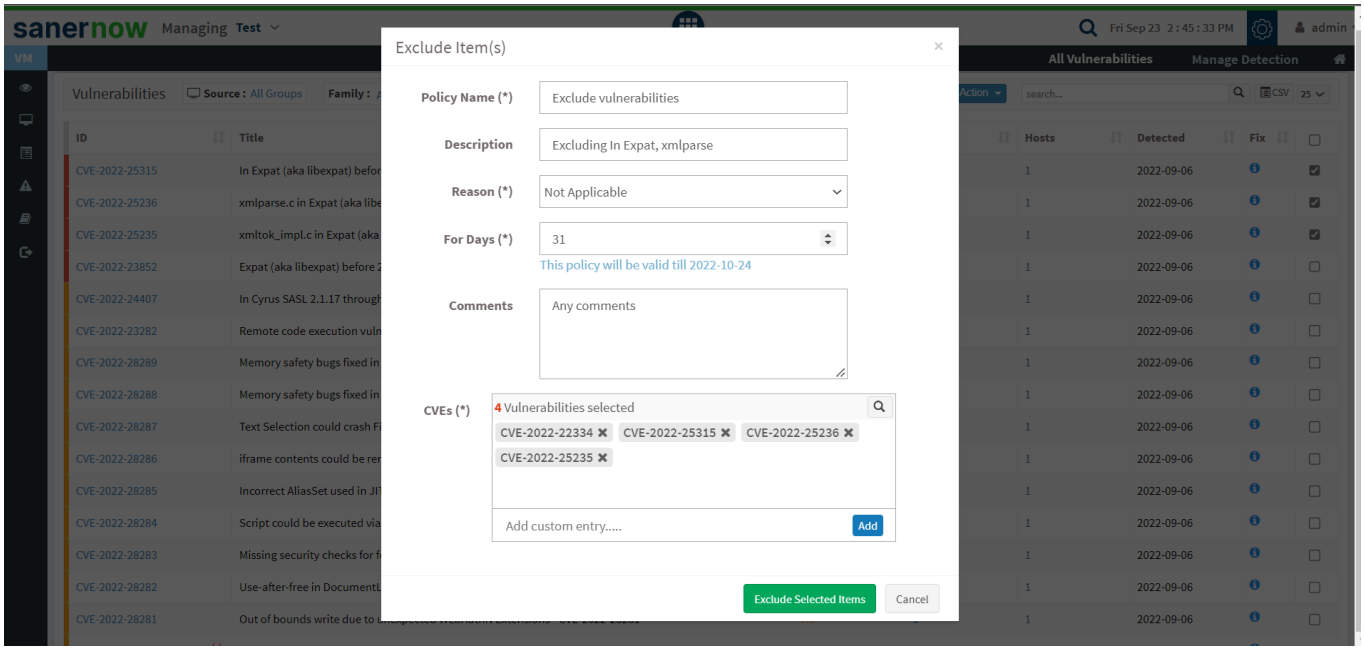


- Select the reason for excluding the vulnerability from the dropdown menu: False Positive, Not Applicable, or Risk Accepted.

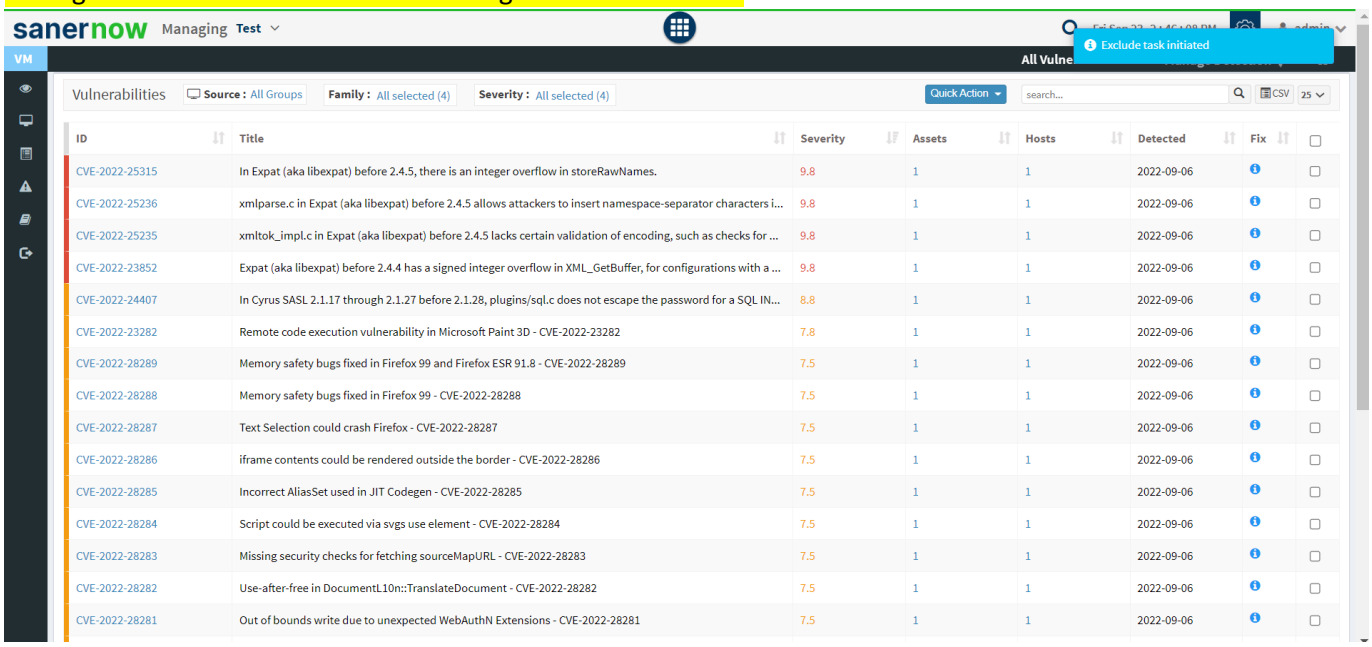


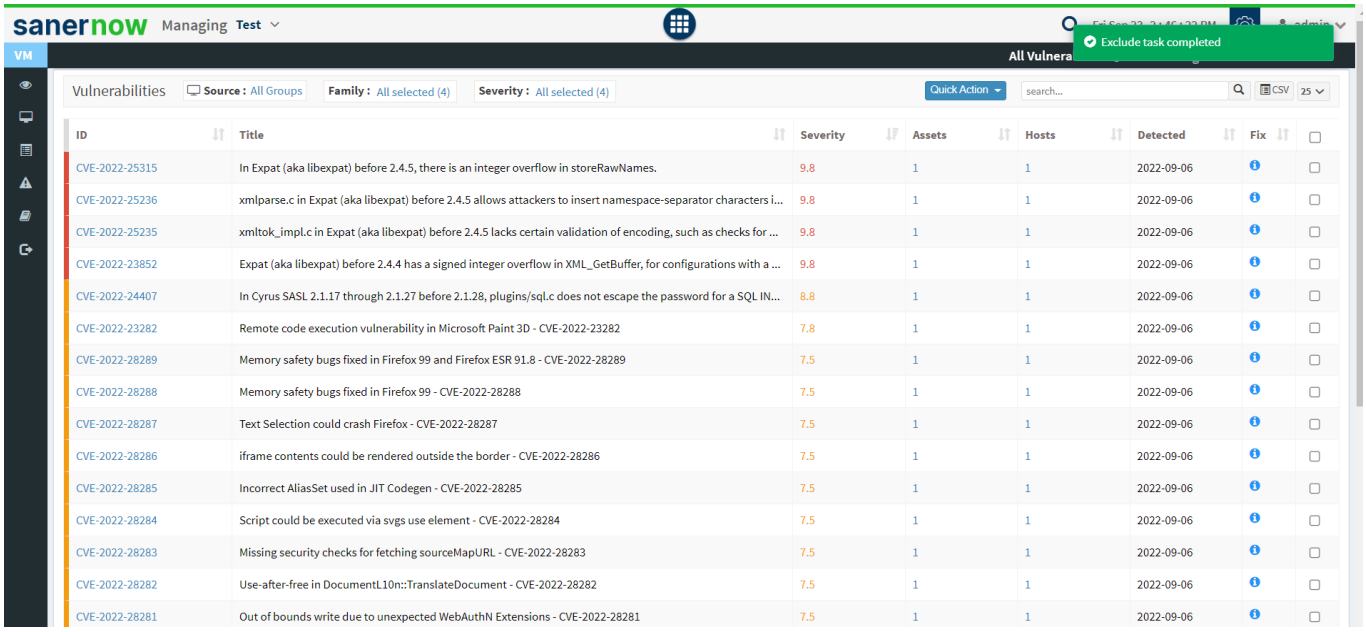
- Assign the number of days you want to exclude (the maximum days for exclusion is 999).
- Give comments if required.
- Apart from the check box, you can custom add the CVEs or USNs for exclusion.



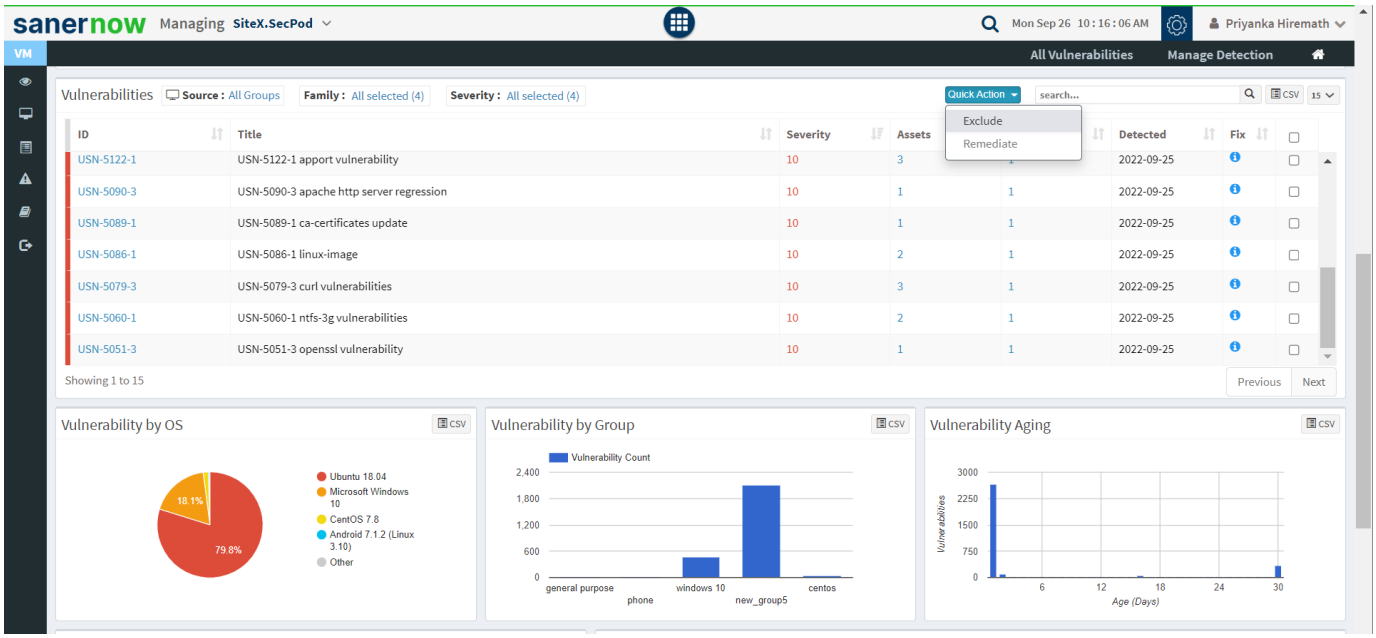


- Click on Exclude Selected Items. The exclude task gets initiated. The excluded vulnerabilities do not show up on the vulnerability dashboard due to the specified policy reason. However, you can view and manage those vulnerabilities in the Manage Detection section.

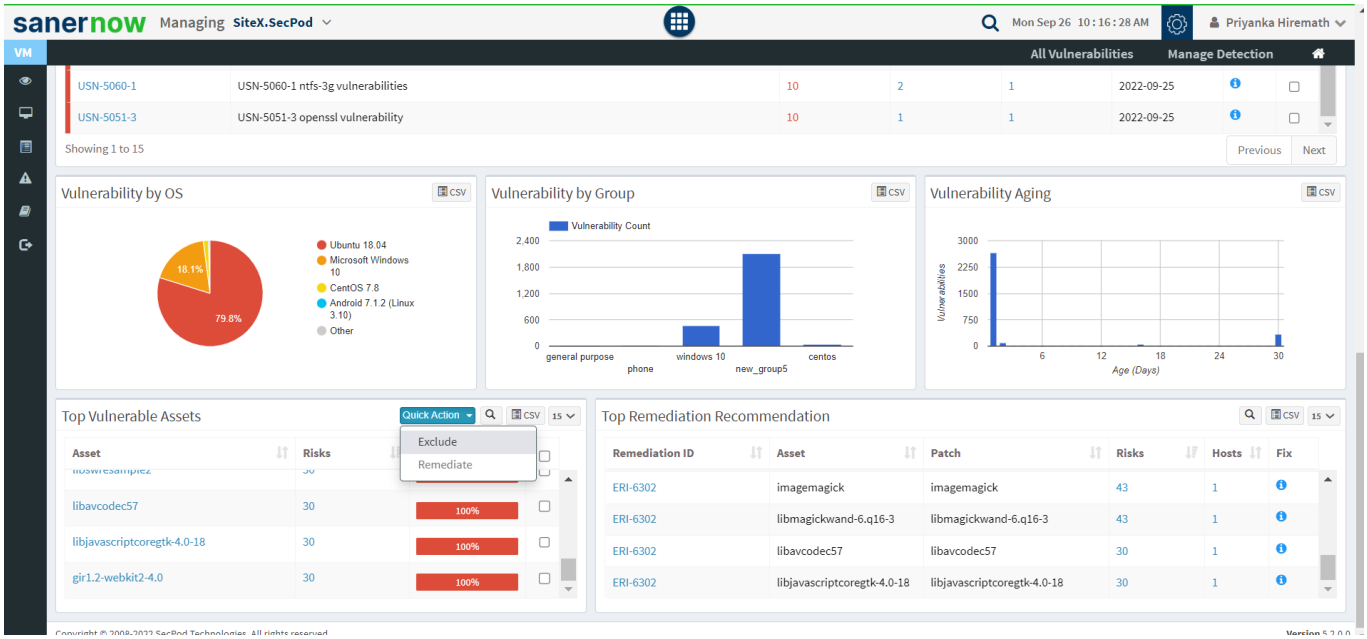




2. You can exclude vulnerabilities from the vulnerabilities panel in the vulnerability management dashboard



3. Also, you can exclude the assets and their vulnerabilities from the Top Vulnerable Assets Panel

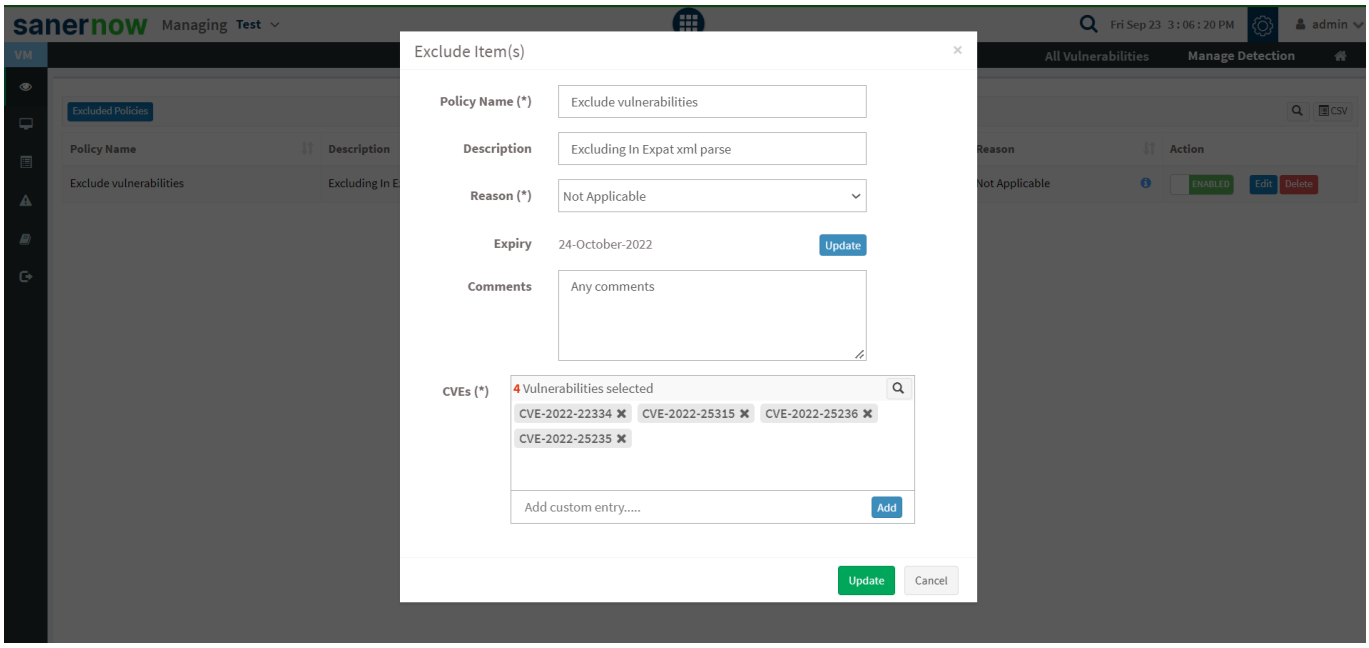


Once you click on exclude, you can fill up all the policy details as explained above and manage excluded vulnerabilities in the Manage Detection section.

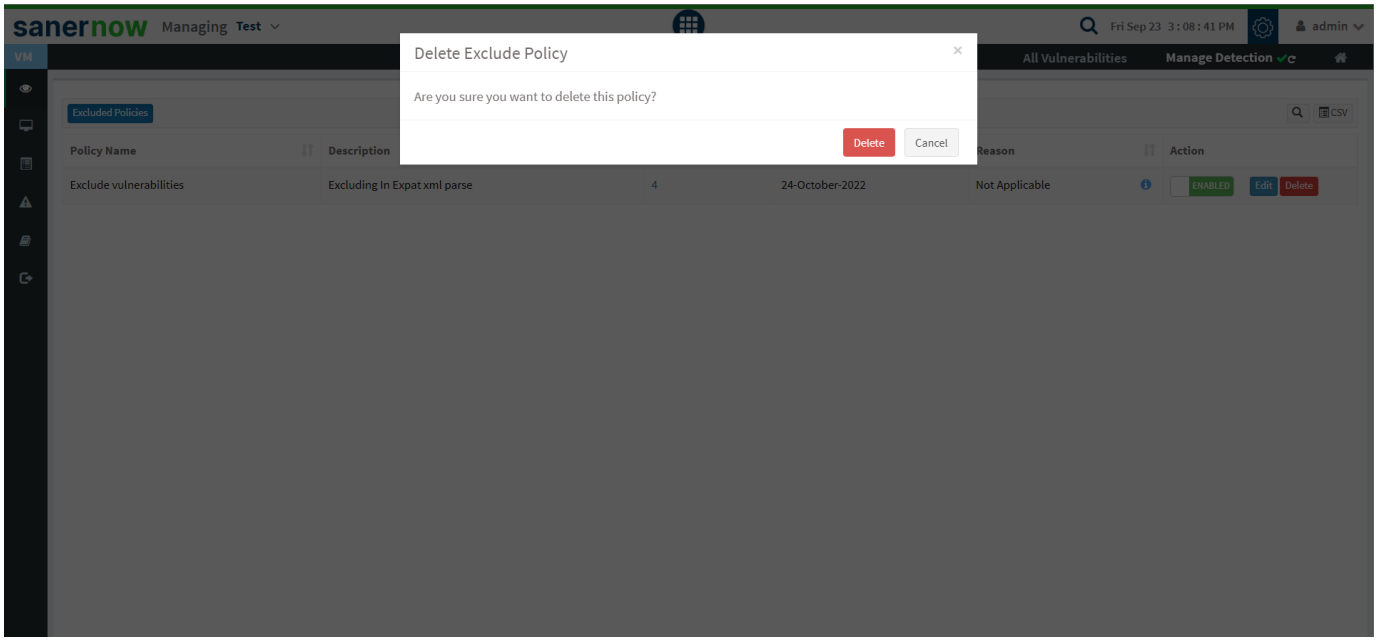
Manage Detection

In Manage Detection, you can view all the excluded policies, edit policies, and delete them from the exclusion list.

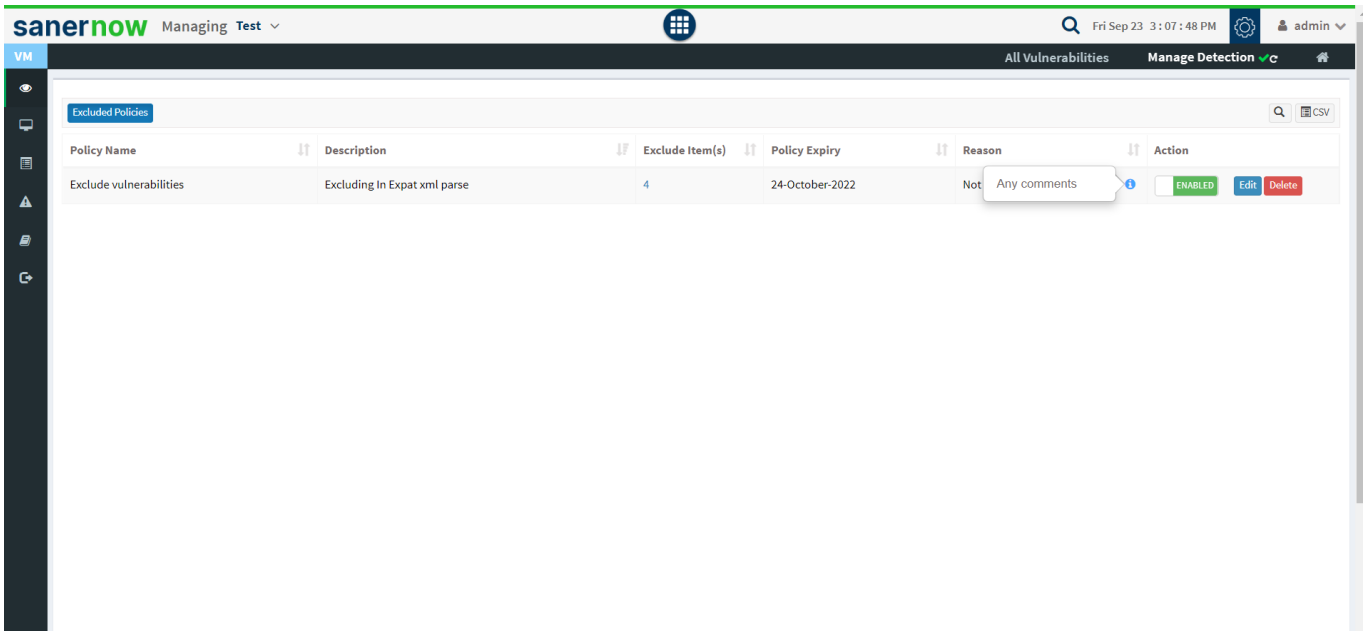
- To edit policies, click on edit in the Action section and fill up all the required policy details in Exclude Item(s) window.



- Click on the Delete button in the Action section to delete the policy.



- In the Action section, you can also enable or disable the policy.
- The (i) icon displays the comment given to the policy.

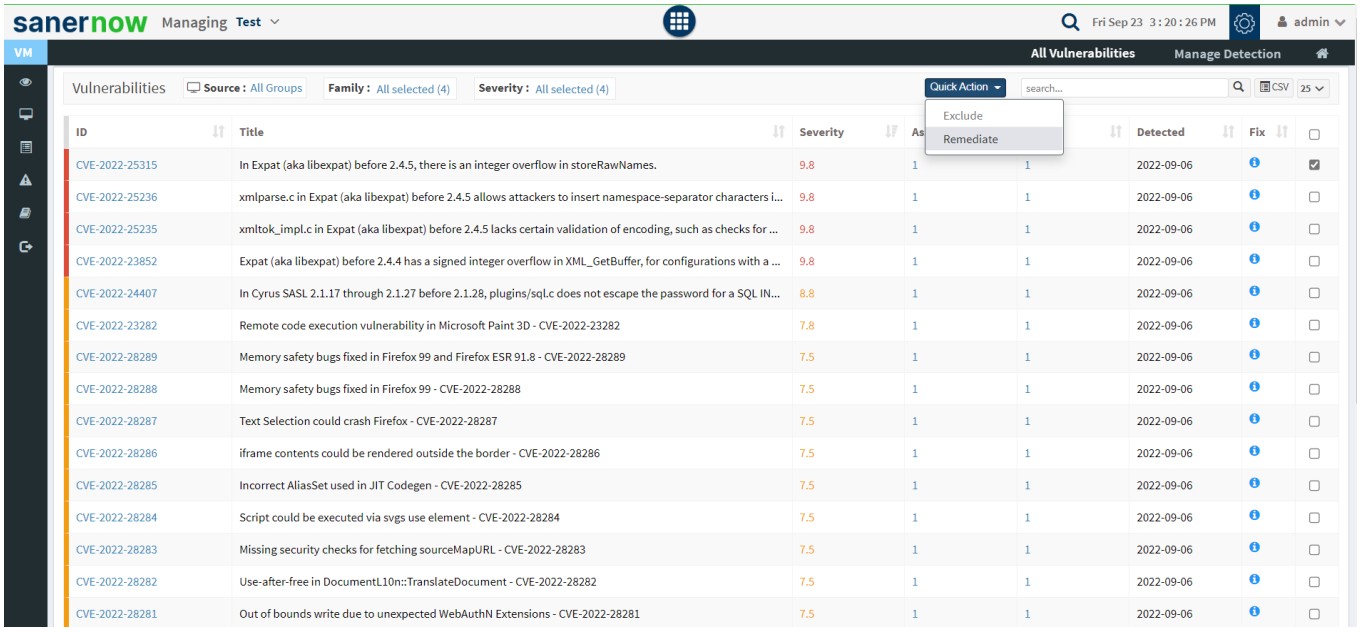


- You can also export the excluded vulnerabilities through CSV.

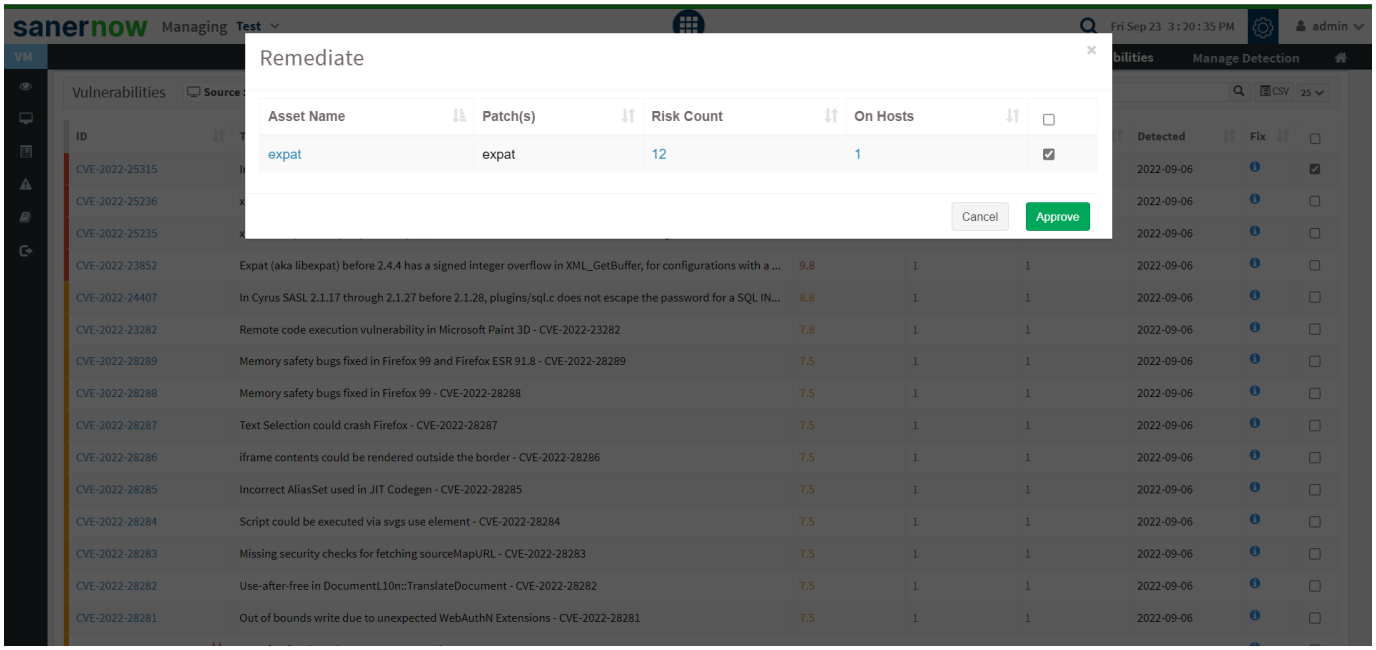
Remediating Vulnerabilities from Vulnerability Management Dashboard:

You can remediate vulnerabilities in three possible ways:

1. **Remediate from All Vulnerability dashboard**
   - In All Vulnerabilities, select the vulnerabilities from the check box to remediate.



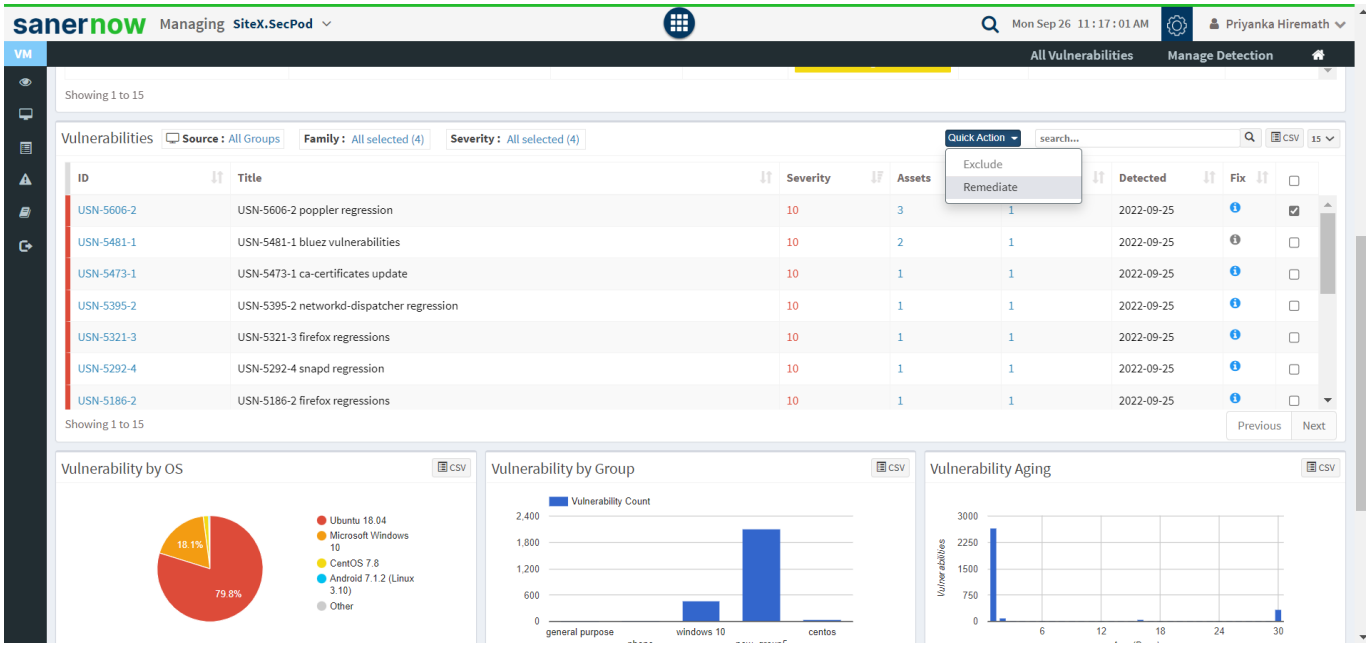
- Click on Quick Action and select Remediate.
- Approve the patches for remediation.

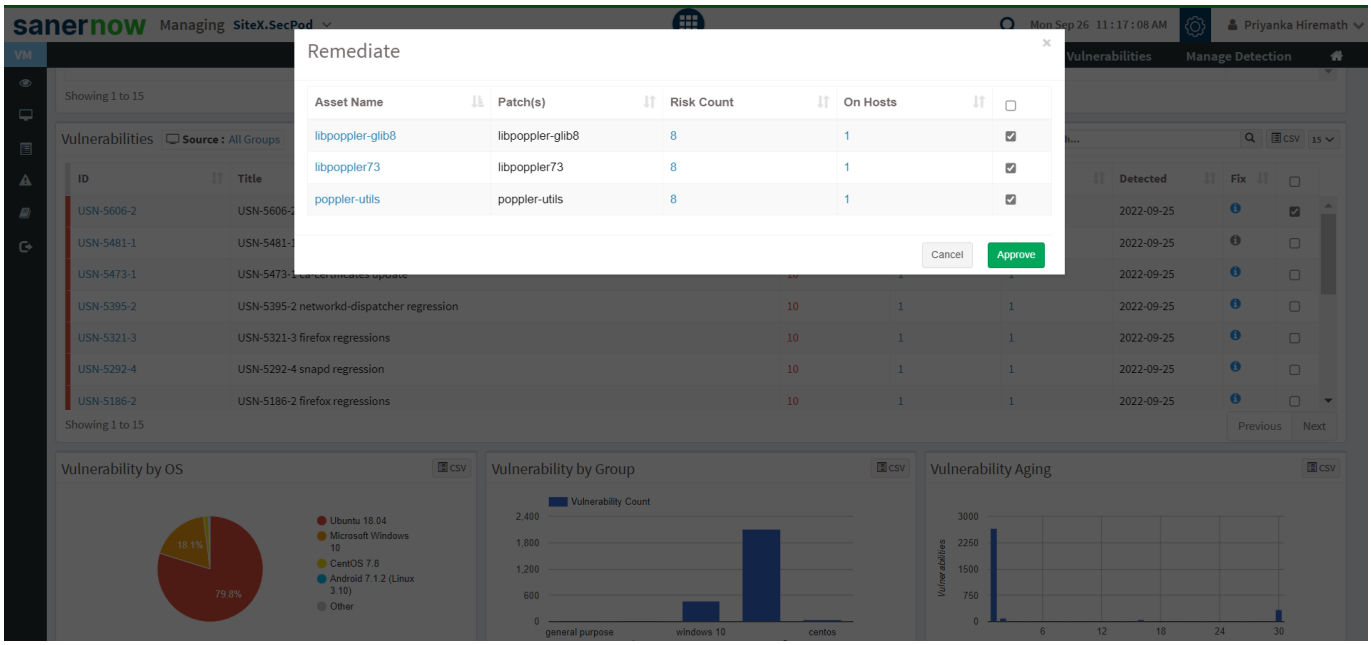


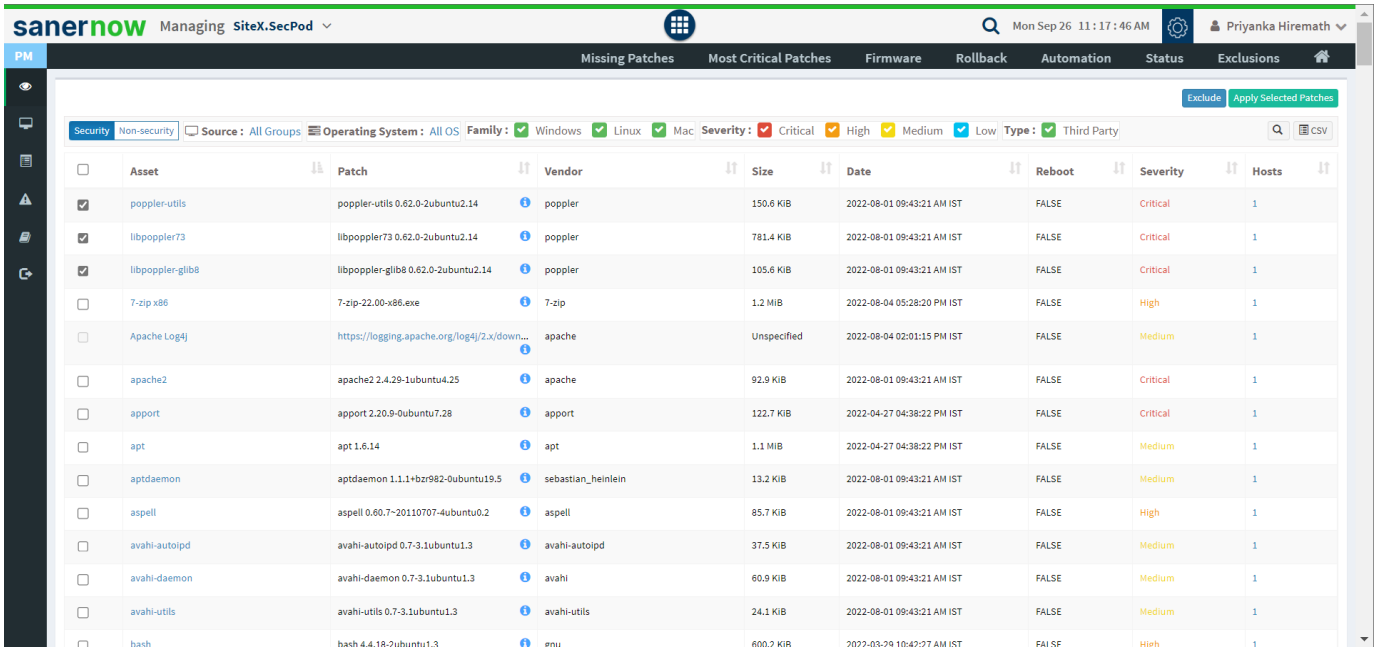
- You will be redirected to the Patch Management module.
- Click on Apply Selected Patches and Create a patching task for remediation.

2. Remediate from the Vulnerabilities panel in the vulnerability management dashboard

- Select the vulnerabilities you want to remediate. Go to quick action and select Remediate and click on approve. You will be redirected to the patch management dashboard.


sanernow
Managing SiteX.SecPod
Mon Sep 26 11:17:01 AM
Priyanka Hiremath
VM
All Vulnerabilities
Manage Detection
Showing 1 to 15
Vulnerabilities
Source : All Groups
Family : All selected (4)
Severity : All selected (4)
Quick Action
Exclude
Remediate
search...
CSV
15
ID
Title
Severity
Assets
Detected
Fix
USN-5606-2
USN-5606-2 poppler regression
USN-5481-1
USN-5481-1 bluez vulnerabilities
USN-5473-1
USN-5473-1 ca-certificates update
USN-5395-2
USN-5395-2 networkd-dispatcher regression
USN-5321-3
USN-5321-3 firefox regressions
USN-5292-4
USN-5292-4 snapd regression
USN-5186-2
USN-5186-2 firefox regressions
2022-09-25
Showing 1 to 15
Previous
Next
Vulnerability by OS
Ubuntu 18.04
Microsoft Windows 10
CentOS 7.8
Android 7.1.2 (Linux 3.10)
Other
18.1%
79.8%
Vulnerability by Group
Vulnerability Count
general purpose
windows 10
centos
Vulnerability Aging
Vulnerabilities

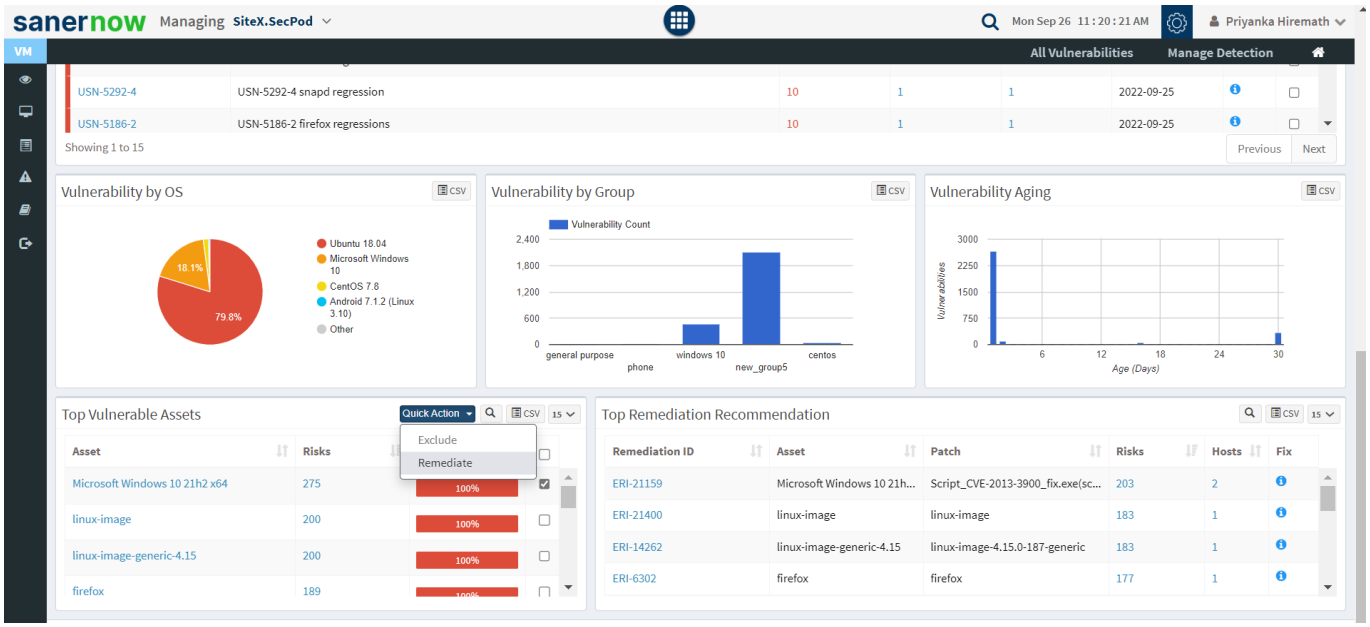

sanernow
Managing SiteX.SecPod
Mon Sep 26 11:17:08 AM
Priyanka Hiremath
Remediate
Asset Name
Patch(s)
Risk Count
On Hosts
libpoppler-glib8
libpoppler-glib8
8
1
libpoppler73
libpoppler73
8
1
poppler-utils
poppler-utils
8
1
Cancel
Approve
Vulnerabilities
Manage Detection
Showing 1 to 15
Vulnerability by OS
Vulnerability by Group
Vulnerability Aging

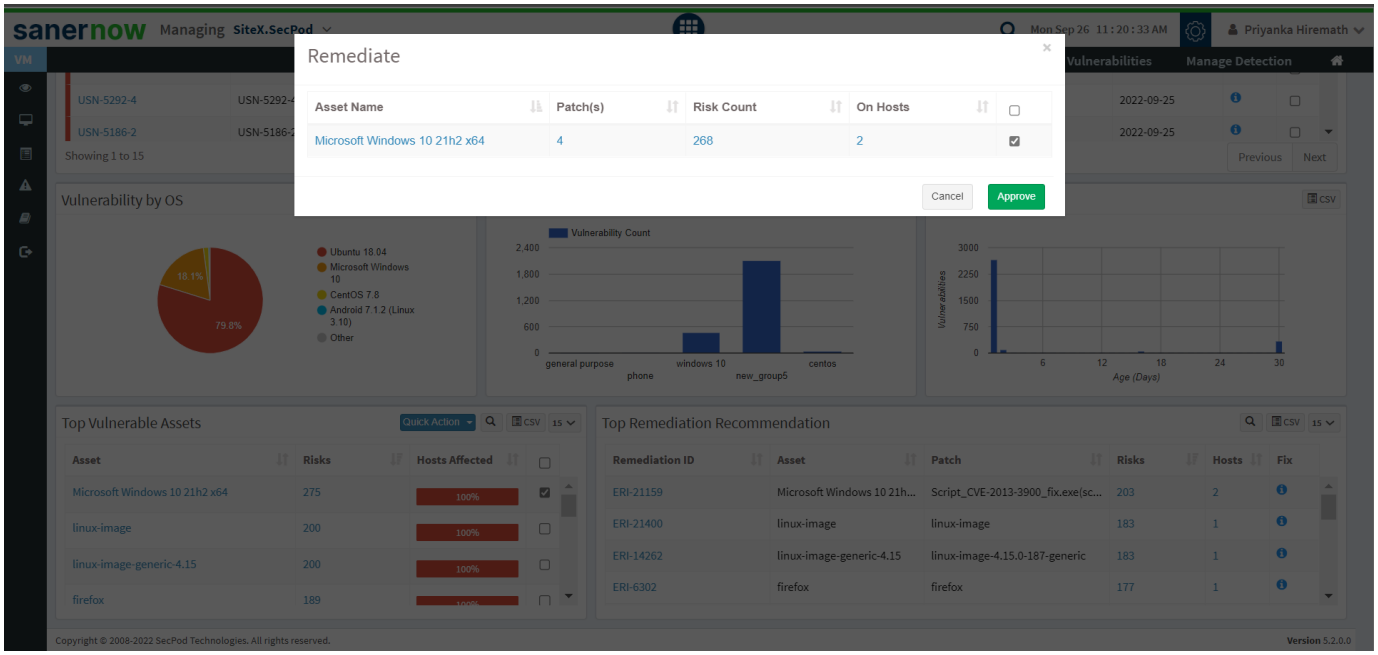


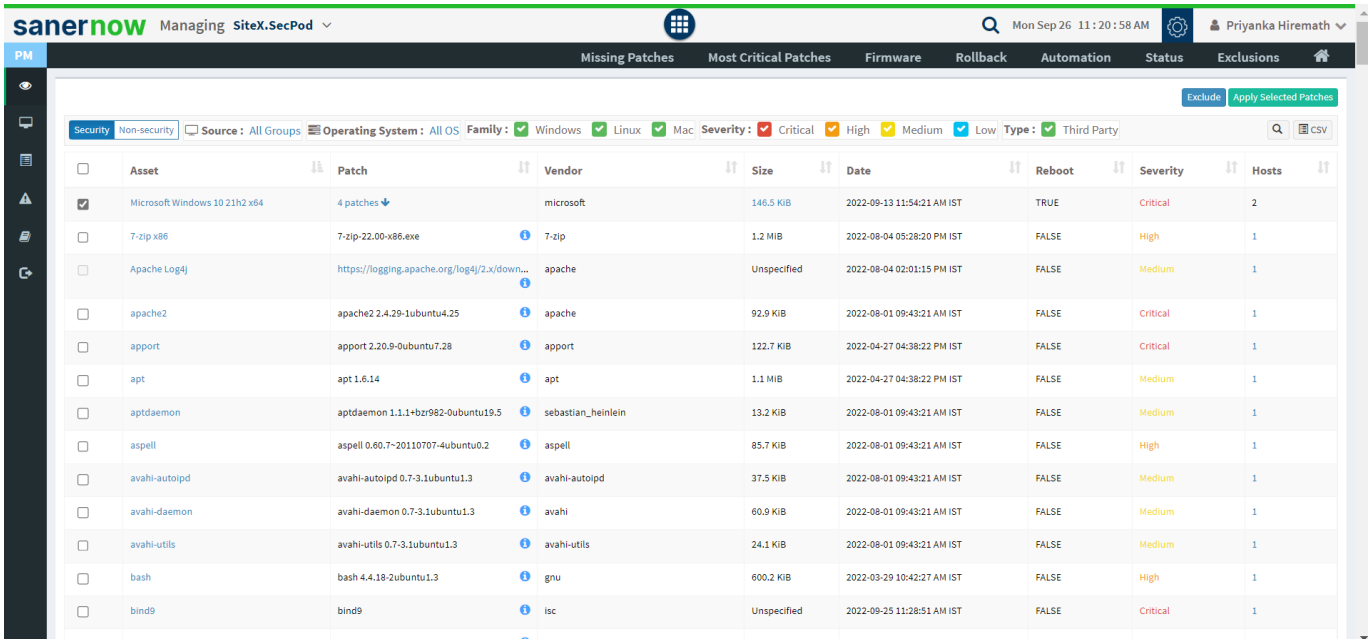
- Click on Apply Selected Patches and create a patching task.

3. Remediate from Top Vulnerable Assets

- Select the assets and click on quick action. The vulnerabilities associated with assets can be remediated.







- Repeat the same procedure as explained above to remediate the vulnerabilities the corresponding assets.

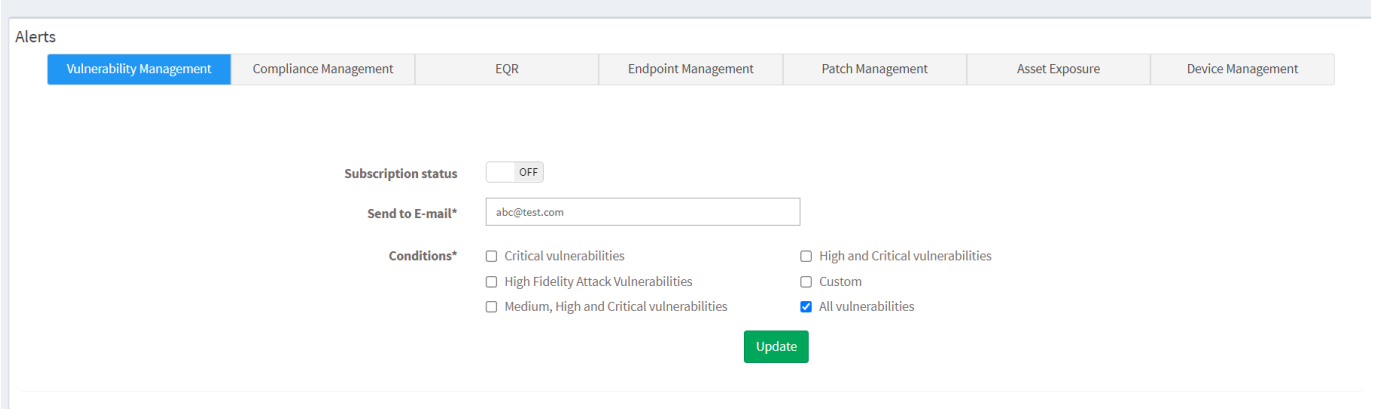
Setting Alerts for Vulnerabilities

The **Alerts** section sends a notification alert to the specified email on the detection of new vulnerabilities after a scheduled scan. This setting must be set before the first scheduled scan. The notification for vulnerabilities is based on their criticality.

To set alerts for vulnerabilities:

- Select the **Alerts** option on the left pane.
- Turn on **Subscription Status** to enable vulnerability alerts.
- Specify an email address to which the alerts will be sent and the category of vulnerability on which notifications will be based. You can also specify a custom condition based on CVEs.

- Click on the **Update** button.



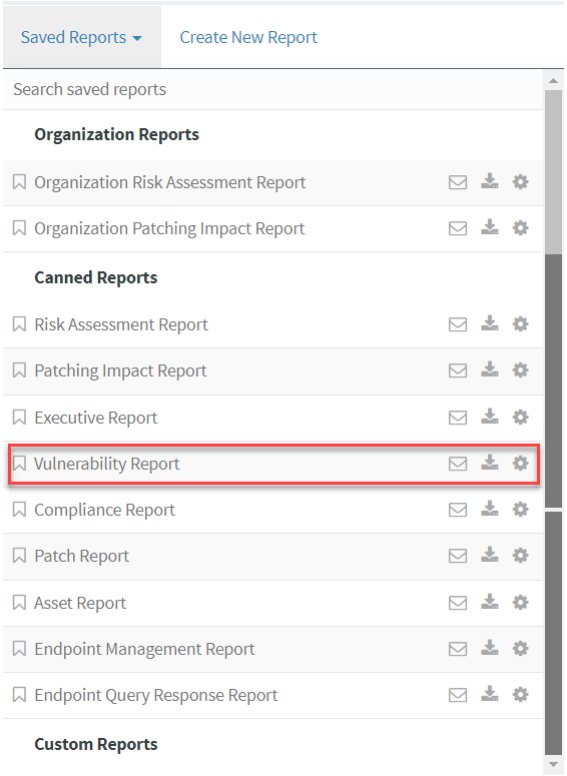
Vulnerability Reports

SanerNow provides an extensive range of reports to understand the vulnerability process. Go to the Reports option on the visibility dashboard to check the reports. You will get two types of reports: Canned reports and customizable reports. Users can access the available vulnerability reports from the Canned reports section.

The user can customize the report by clicking on the Create New Report option. Select a vulnerability report builder APIs and drag them to the Custom Report page to build a new report. Once the report is created, save, and configure a backup for that report.

To Generate the Endpoint Management Report

- Click **Reports > Saved Reports > Vulnerability Report**.



To export the report to a PDF.

- Click on the download icon beside the vulnerability report to download the PDF report.

To export the report and send it via email

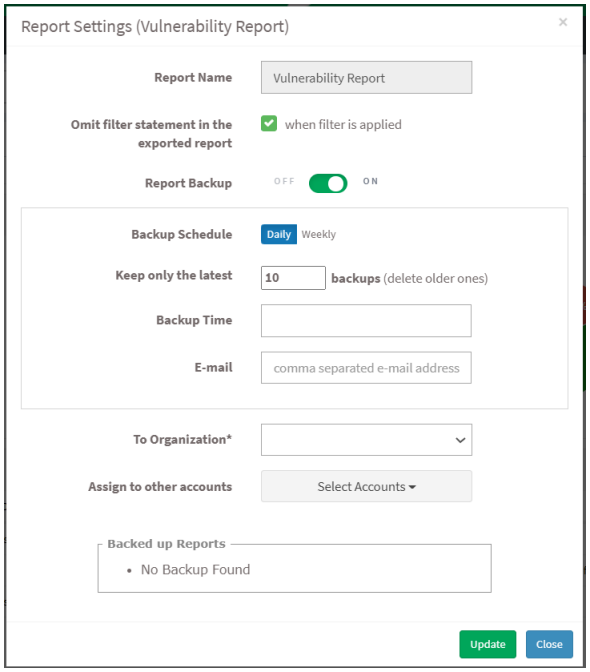
- Click on the **Mail** icon in the saved report section to email the report.
- Specify the email addresses.

To Backup Vulnerability Reports

The backup settings under **Reports** allow IT, administrators, to obtain a report backup. The report backup can be scheduled daily or weekly to run automatically.

To configure backup settings for reports:

- Click the **Reports** option on the left pane.
- Click the **Saved Reports > Canned Reports > Vulnerability Report**.
- Select the **Settings** icon beside the Vulnerability Report.
- Report Settings (Vulnerability Report) pop up will be displayed.



- Click the **Omit filter statement in the exported report** check box, and you can set the on/off button to back up the report or not.
- If the backup is on, select the weekly or daily option.
- Set a number in the **Keep only the latest** entry box. The report for the specified number of days is archived. If the number is three and the backup option is daily, then the reports from the last three days are maintained. Older files are deleted. You can maintain backups for a maximum of 30 days.
- Specify **Email ID** address. You can enter more than one email address comma separated.
- Select the organization and accounts you want to apply these settings.
- Click on the **Save** button.

About SecPod, Inc.

SecPod is a leading provider of endpoint security and management solutions. SecPod (Security Podium, incarnated as SecPod) has created a revolutionary SanerNow platform and tools used by MSPs and enterprises worldwide. SecPod also licenses security technology to top security vendors through its SCAP Content Professional Feed.

303 Twin Dolphin Drive,

6th Floor, Redwood City,

California 94065, USA.

To learn more about SecPod, visit:

www.SecPod.com

Contact

Sales : info@secpod.com

Support : support@secpod.com

Phone : (+1) 918 625 3023 (US)