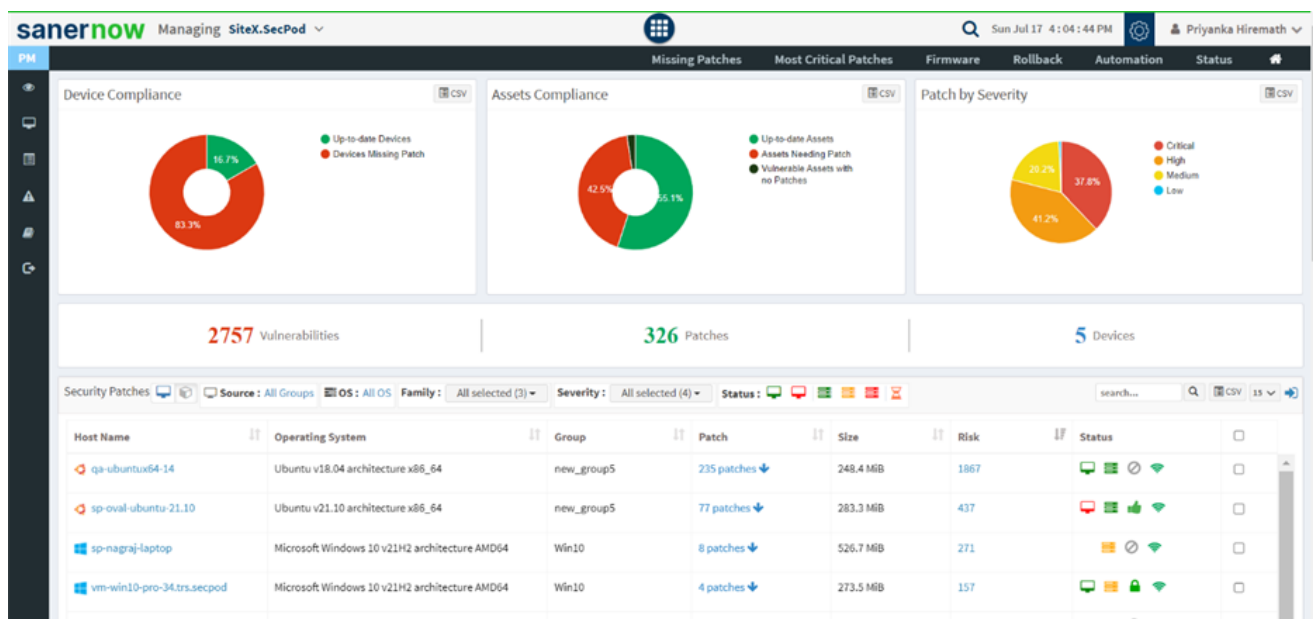


How to apply the most critical patches in SanerNow?

SanerNow lists the most critical patches and allows remediation for the same. Let us learn how to apply the most critical patches in SanerNow.

1. In Sanernow, go to the **Patch Management dashboard**.



2. In the patch management dashboard, click on **Most Critical Patches**.
3. You will be displayed with all the missing patches, assigned vendor, asset name, patch size, and other details.

sanernow Managing SiteX.SecPod

Tue Jul 19 2:58:07 PM Priyanka Hiremath

Missing Patches Most Critical Patches Firmware Rollback Automation Status

Asset Source: All Groups Operating System: All OS Asset Family: Windows Linux Mac

| Asset | Patch | Vendor | Size | Date | Reboot | High Fidelity Attacks | Hosts |
|--|---|-----------------------------|-------------|----------------------------|--------|---|-------|
| <input checked="" type="checkbox"/> apache2 | apache2 2.4.29-1ubuntu4.25 | apache | 92.9 KIB | 2022-06-16 01:54:57 PM UTC | FALSE | Apache HTTP Server Active Exploits | 1 |
| <input checked="" type="checkbox"/> firefox | firefox 100.0.2-build1-0ubuntu0.21.10.1 | mozilla | 60.3 MIB | 2022-04-27 11:08:22 AM UTC | FALSE | Tails Active Exploits,Firefox Active Exploits,... | 2 |
| <input type="checkbox"/> glibc-javascriptcoregtk-4.0 | glibc-javascriptcoregtk-4.0 2.36.2-0ubuntu... | glibc-javascriptcoregtk-4.0 | 30.0 KIB | 2022-06-01 08:06:04 AM UTC | FALSE | ScamClub Group,DazzleSpy Spyware,Apple... | 1 |
| <input type="checkbox"/> glibc-webkit2-4.0 | glibc-webkit2-4.0 2.36.2-0ubuntu0.21.10.1 | glibc-webkit2-4.0 | 89.4 KIB | 2022-06-01 08:06:04 AM UTC | FALSE | ScamClub Group,DazzleSpy Spyware,Apple... | 1 |
| <input type="checkbox"/> Google Chrome | google-chrome-109.0.5090.114-64-deb.deb | google | 81.9 MIB | 2022-06-02 05:03:25 AM UTC | FALSE | Google Chrome Active Exploits,RedLine Mal... | 1 |
| <input type="checkbox"/> intel-microcode | intel-microcode 3.20220510.0ubuntu0.18.0... | intel-microcode | 3.9 MIB | 2022-06-16 01:54:58 PM UTC | FALSE | Spectre | 1 |
| <input type="checkbox"/> libjavascriptcoregtk-4.0-18 | libjavascriptcoregtk-4.0-18 2.32.4-0ubuntu... | webkitgtk | 5.5 MIB | 2022-04-27 11:08:22 AM UTC | FALSE | ScamClub Group,DazzleSpy Spyware,Apple... | 1 |
| <input type="checkbox"/> libwebkit2gtk-4.0-37 | libwebkit2gtk-4.0-37 2.32.4-0ubuntu0.18.04.1 | webkitgtk | 12.8 MIB | 2022-04-27 11:08:22 AM UTC | FALSE | ScamClub Group,DazzleSpy Spyware,Apple... | 1 |
| <input type="checkbox"/> linux-image-generic-5.13 | linux-image-5.13.0-35-generic | linux | Unspecified | 2022-06-01 08:06:04 AM UTC | TRUE | Dirty Pipe | 1 |
| <input type="checkbox"/> Microsoft Windows 10 21H2 x64 | 2 patches | microsoft | 0 B | 2022-07-12 05:52:52 PM UTC | TRUE | Microsoft Windows Active Exploits, Follina, ... | 1 |
| <input type="checkbox"/> sudo | sudo 1.8.21p0-0ubuntu1.4 | todd_miller | 418.3 KIB | 2022-06-16 01:54:58 PM UTC | FALSE | Baron Samedi | 1 |
| <input type="checkbox"/> thunderbird | thunderbird 151.9.1-build1-0ubuntu0.18.0... | mozilla | 53.0 MIB | 2022-04-27 11:08:22 AM UTC | FALSE | Tails Active Exploits | 2 |

4. Set up the Asset source, Operating systems, and Asset family.

sanernow Managing SiteX.SecPod

Tue Jul 19 2:59:26 PM Priyanka Hiremath

Missing Patches Firmware Rollback Automation Status

Asset Source: All Groups

Select Groups/Devices

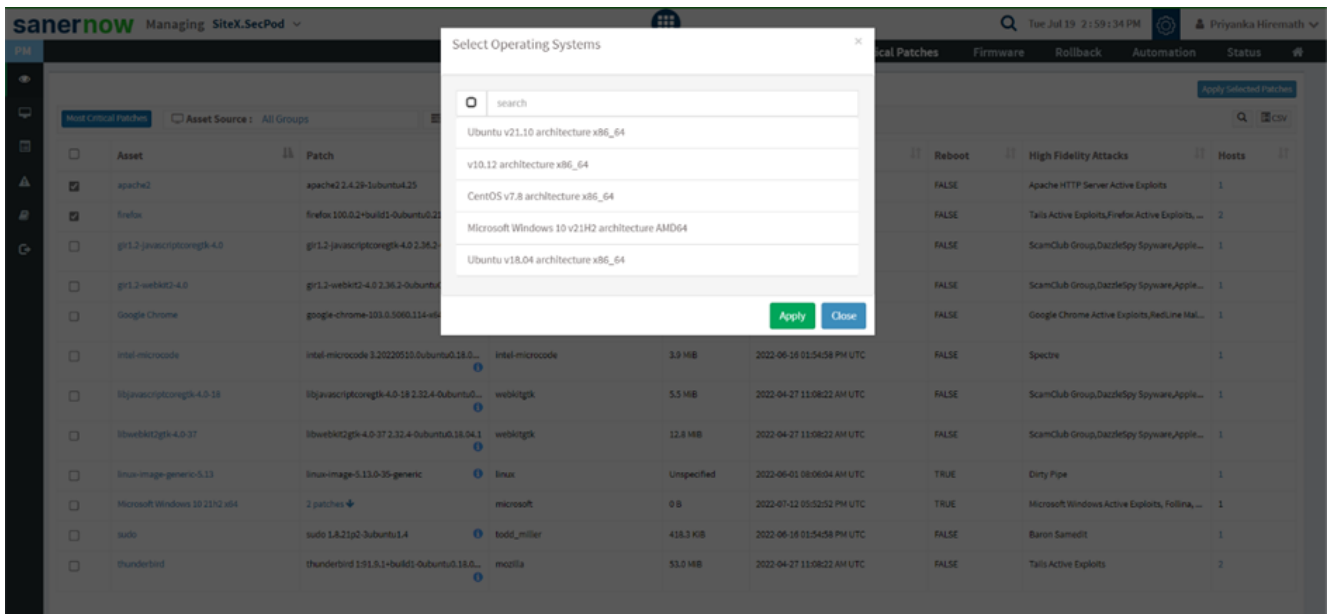
Device: ☒ Active ☒ Inactive

Type here to search...

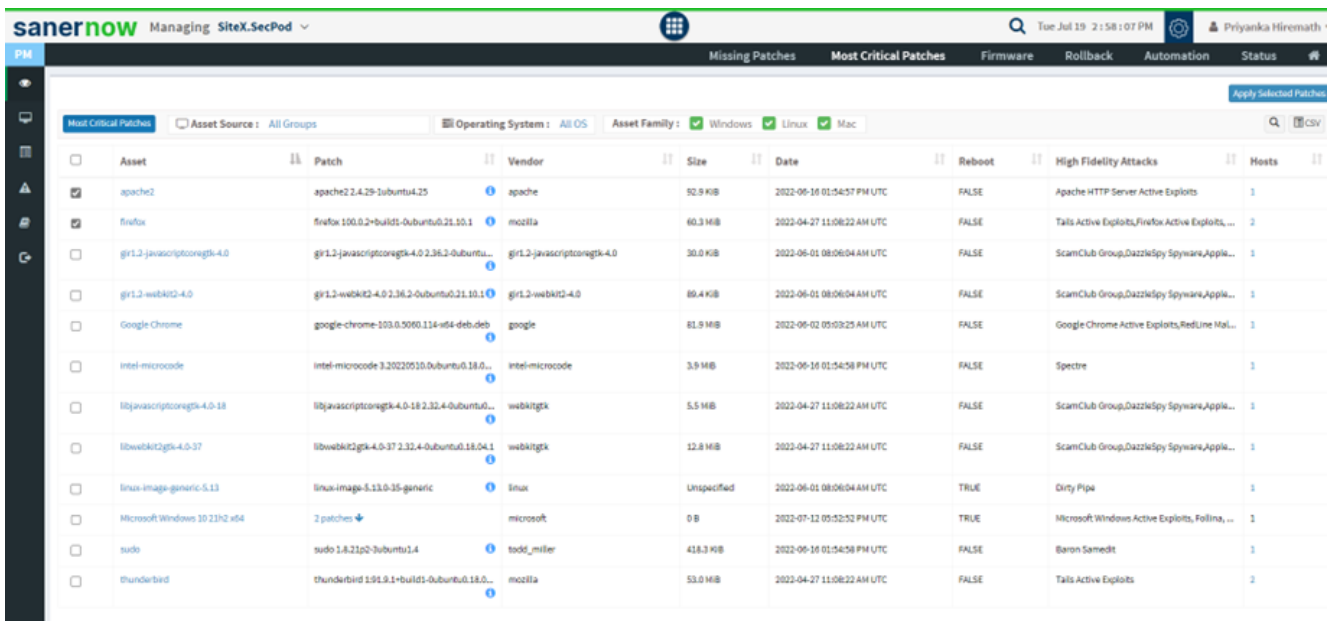
- ☒ centos
 - ☒ sp-centos-7-x64
- ☐ mac os
- ☒ new_group5
 - ☒ qe-ubuntu64-14
 - ☐ sp-oval-ubuntu-21.10
- ☒ Win10
 - ☒ sp-nagray-laptop
 - ☐ vm-win10-pro-34.tris.secpod

Apply Close

| Asset | Patch | Vendor | Size | Date | Reboot | High Fidelity Attacks | Hosts |
|--|---|-----------------------------|-------------|----------------------------|--------|---|-------|
| <input checked="" type="checkbox"/> apache2 | apache2 2.4.29-1ubuntu4.25 | apache | 92.9 KIB | 2022-06-16 01:54:57 PM UTC | FALSE | Apache HTTP Server Active Exploits | 1 |
| <input checked="" type="checkbox"/> firefox | firefox 100.0.2-build1-0ubuntu0.21.10.1 | mozilla | 60.3 MIB | 2022-04-27 11:08:22 AM UTC | FALSE | Tails Active Exploits,Firefox Active Exploits,... | 2 |
| <input type="checkbox"/> glibc-javascriptcoregtk-4.0 | glibc-javascriptcoregtk-4.0 2.36.2-0ubuntu... | glibc-javascriptcoregtk-4.0 | 30.0 KIB | 2022-06-01 08:06:04 AM UTC | FALSE | ScamClub Group,DazzleSpy Spyware,Apple... | 1 |
| <input type="checkbox"/> glibc-webkit2-4.0 | glibc-webkit2-4.0 2.36.2-0ubuntu0.21.10.1 | glibc-webkit2-4.0 | 89.4 KIB | 2022-06-01 08:06:04 AM UTC | FALSE | ScamClub Group,DazzleSpy Spyware,Apple... | 1 |
| <input type="checkbox"/> Google Chrome | google-chrome-109.0.5090.114-64-deb.deb | google | 81.9 MIB | 2022-06-02 05:03:25 AM UTC | FALSE | Google Chrome Active Exploits,RedLine Mal... | 1 |
| <input type="checkbox"/> intel-microcode | intel-microcode 3.20220510.0ubuntu0.18.0... | intel-microcode | 3.9 MIB | 2022-06-16 01:54:58 PM UTC | FALSE | Spectre | 1 |
| <input type="checkbox"/> libjavascriptcoregtk-4.0-18 | libjavascriptcoregtk-4.0-18 2.32.4-0ubuntu... | webkitgtk | 5.5 MIB | 2022-04-27 11:08:22 AM UTC | FALSE | ScamClub Group,DazzleSpy Spyware,Apple... | 1 |
| <input type="checkbox"/> libwebkit2gtk-4.0-37 | libwebkit2gtk-4.0-37 2.32.4-0ubuntu0.18.04.1 | webkitgtk | 12.8 MIB | 2022-04-27 11:08:22 AM UTC | FALSE | ScamClub Group,DazzleSpy Spyware,Apple... | 1 |
| <input type="checkbox"/> linux-image-generic-5.13 | linux-image-5.13.0-35-generic | linux | Unspecified | 2022-06-01 08:06:04 AM UTC | TRUE | Dirty Pipe | 1 |
| <input type="checkbox"/> Microsoft Windows 10 21H2 x64 | 2 patches | microsoft | 0 B | 2022-07-12 05:52:52 PM UTC | TRUE | Microsoft Windows Active Exploits, Follina, ... | 1 |
| <input type="checkbox"/> sudo | sudo 1.8.21p0-0ubuntu1.4 | todd_miller | 418.3 KIB | 2022-06-16 01:54:58 PM UTC | FALSE | Baron Samedi | 1 |
| <input type="checkbox"/> thunderbird | thunderbird 151.9.1-build1-0ubuntu0.18.0... | mozilla | 53.0 MIB | 2022-04-27 11:08:22 AM UTC | FALSE | Tails Active Exploits | 2 |



5. Now select the assets that you want to patch.



6. Click on **Apply Selected Patches**.

sanernow Managing SiteX.SecPod

Tue Jul 19 2:58:07 PM Priyanka Hiremath

Missing Patches Most Critical Patches Firmware Rollback Automation Status

Most Critical Patches Asset Source: All Groups Operating System: All OS Asset Family: Windows Linux Mac

| Asset | Patch | Vendor | Size | Date | Reboot | High Fidelity Attacks | Hosts |
|--|--|---------------------------|-------------|----------------------------|--------|---|-------|
| <input checked="" type="checkbox"/> apache2 | apache2 2.4.29-1ubuntu4.25 | apache | 92.9 KIB | 2022-06-16 01:54:57 PM UTC | FALSE | Apache HTTP Server Active Exploits | 1 |
| <input checked="" type="checkbox"/> firefox | firefox 100.0.2-build1-0ubuntu0.21.10.1 | mozilla | 60.3 MiB | 2022-04-27 11:08:22 AM UTC | FALSE | Tails Active Exploits, Firefox Active Exploits, ... | 2 |
| <input type="checkbox"/> glibc-javascrptcoregk-4.0 | glibc-javascrptcoregk-4.0 2.36.2-0ubuntu... | glibc-javascrptcoregk-4.0 | 30.0 KIB | 2022-06-01 08:06:04 AM UTC | FALSE | ScamClub Group, DazzleSpy Spyware, Apple... | 1 |
| <input type="checkbox"/> glibc-webkit2-4.0 | glibc-webkit2-4.0 2.36.2-0ubuntu0.21.10.1 | glibc-webkit2-4.0 | 89.4 KIB | 2022-06-01 08:06:04 AM UTC | FALSE | ScamClub Group, DazzleSpy Spyware, Apple... | 1 |
| <input type="checkbox"/> Google Chrome | google-chrome 103.0.5000.114-0deb-deb | google | 81.9 MiB | 2022-06-02 05:03:25 AM UTC | FALSE | Google Chrome Active Exploits, RedLine Mal... | 1 |
| <input type="checkbox"/> intel-microcode | intel-microcode 3.20220510.0ubuntu0.18.0... | intel-microcode | 3.9 MiB | 2022-06-16 01:54:58 PM UTC | FALSE | Spectre | 1 |
| <input type="checkbox"/> libjavascrptcoregk-4.0-18 | libjavascrptcoregk-4.0-18 2.32.4-0ubuntu... | webkitgtk | 5.5 MiB | 2022-04-27 11:08:22 AM UTC | FALSE | ScamClub Group, DazzleSpy Spyware, Apple... | 1 |
| <input type="checkbox"/> libwebkit2gtk-4.0-37 | libwebkit2gtk-4.0-37 2.32.4-0ubuntu0.18.0... | webkitgtk | 12.8 MiB | 2022-04-27 11:08:22 AM UTC | FALSE | ScamClub Group, DazzleSpy Spyware, Apple... | 1 |
| <input type="checkbox"/> linux-image-generic-5.13 | linux-image-5.13.0-35-generic | linux | Unspecified | 2022-06-01 08:06:04 AM UTC | TRUE | Dirty Pipe | 1 |
| <input type="checkbox"/> Microsoft Windows 10 22H2 x64 | 2 patches | microsoft | 0 B | 2022-07-12 05:52:52 PM UTC | TRUE | Microsoft Windows Active Exploits, Pollina... | 1 |
| <input type="checkbox"/> sudo | sudo 1.8.21p2-3ubuntu1.4 | todd_miller | 418.3 KIB | 2022-06-16 01:54:58 PM UTC | FALSE | Baron Samedi | 1 |
| <input type="checkbox"/> thunderbird | thunderbird 159.8.1-build1-0ubuntu0.18.0... | mozilla | 53.0 MiB | 2022-04-27 11:08:22 AM UTC | FALSE | Tails Active Exploits | 2 |

7. Here, assign the task name and schedule the remediation time.

- You can immediately apply patches.

sanernow Managing SiteX.SecPod

Tue Jul 19 3:25:53 PM Priyanka Hiremath

Create Patching Task

Task Controls

- Reboot Control
- Remediation End Time
- Patching Notification
- Remediation Scripts
- Test and Deploy

Task Name

Apply critical patches

Remediation Schedule

Immediate

Task Impact

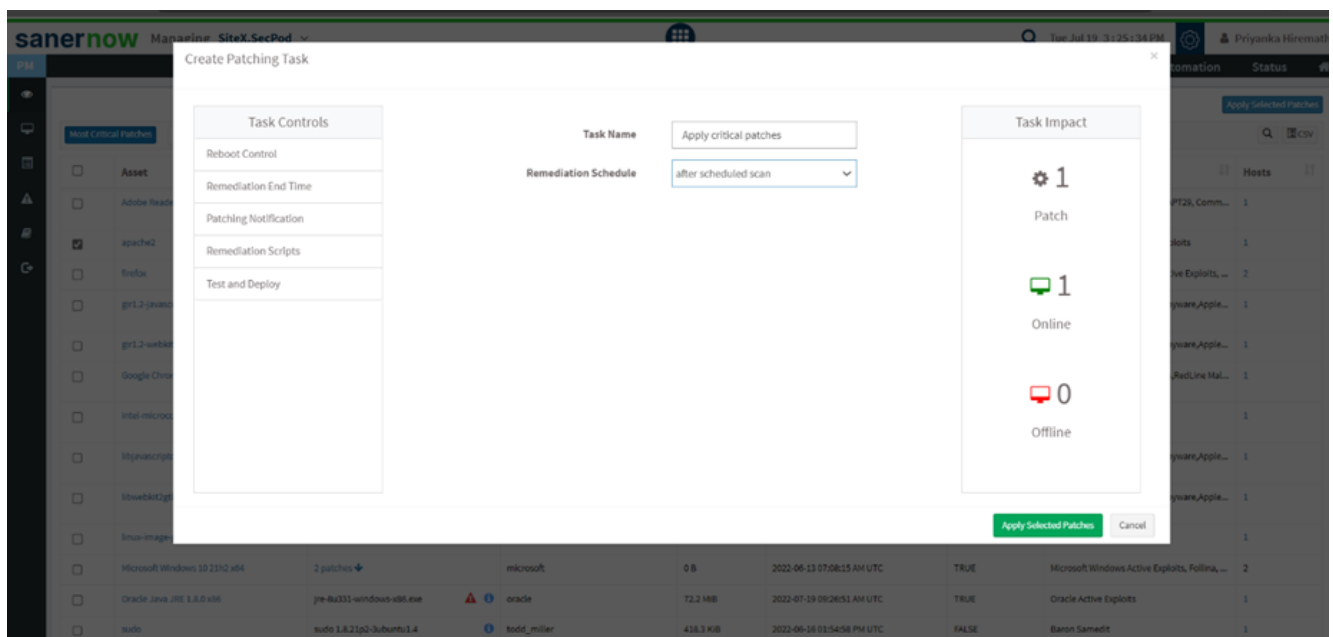
1 Patch

1 Online

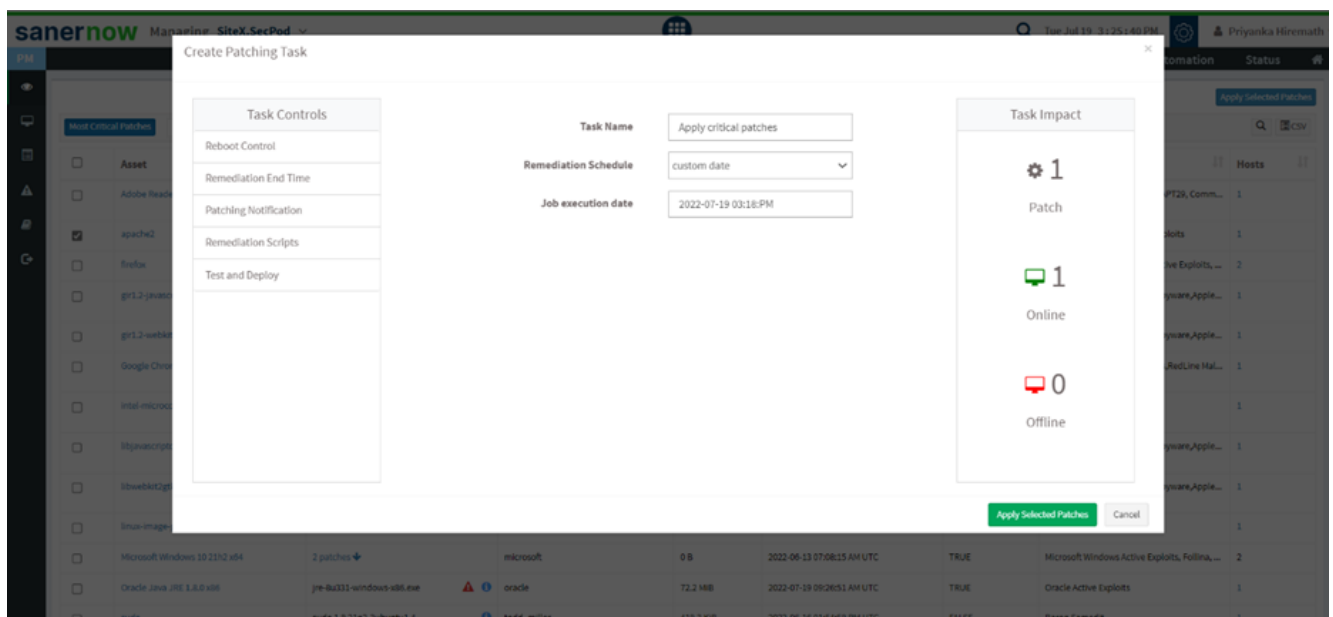
0 Offline

Apply Selected Patches Cancel

- You can apply patches after the scheduled scan

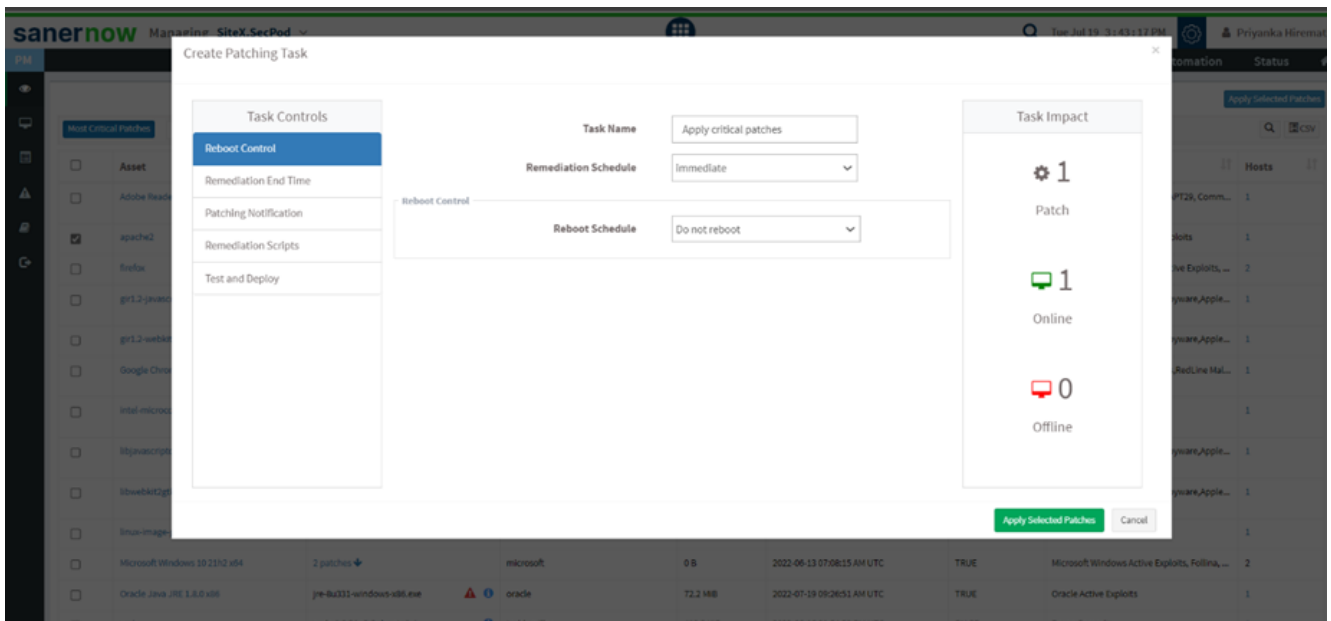


- You can apply patches on a custom date



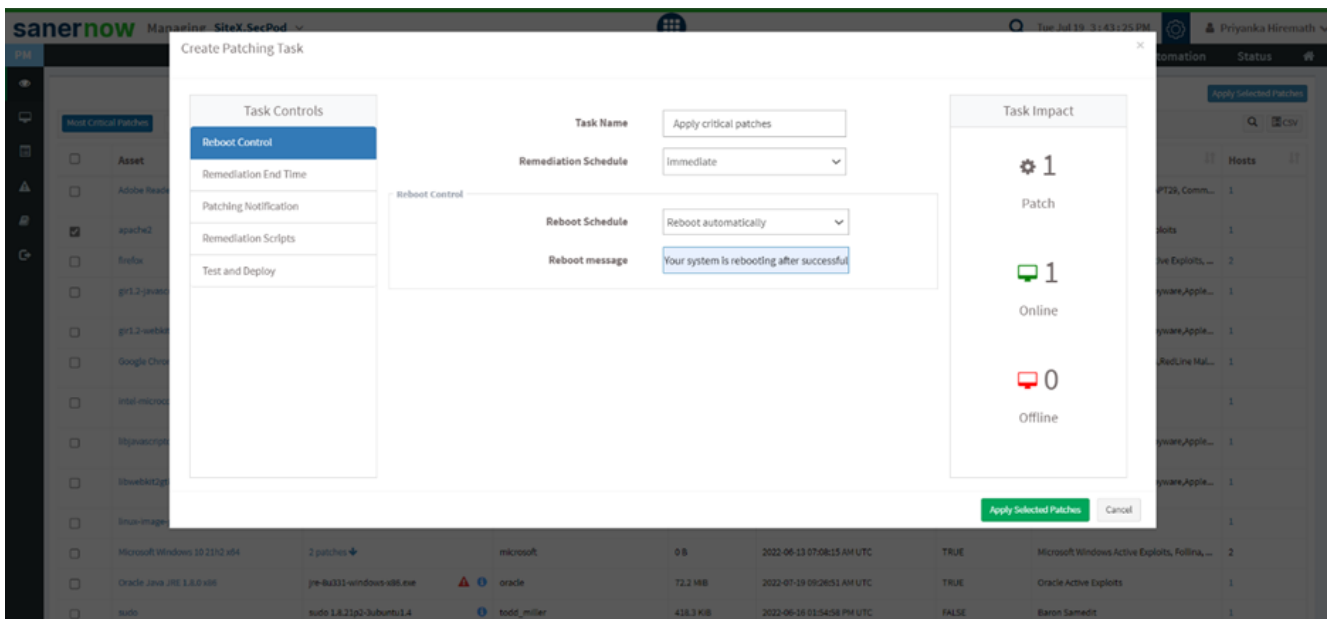
8. You can schedule the reboot time from the **Reboot control** option.

- Do not reboot



- Reboot automatically

Once the patch is applied, the system gets rebooted automatically with a prior reboot notification



- Schedule date and time

You can schedule a date and time with a reboot message.

Create Patching Task

Task Controls

- Reboot Control
- Remediation End Time
- Patching Notification
- Remediation Scripts
- Test and Deploy

Task Name: Apply critical patches

Remediation Schedule: Immediate

Reboot Control

Reboot Schedule: Schedule date and time

Reboot date time: 2022-07-19 12:00AM

Reboot message: Your system is rebooting after successful

Task Impact

- 1 Patch
- 1 Online
- 0 Offline

Assets and Patches Table

| Asset | Patch | Vendor | Size | Created | Status | Details |
|-------------------------------|---------------------------|-------------|----------|----------------------------|--------|---|
| Microsoft Windows 10 21H2 x64 | 2 patches | microsoft | 0 B | 2022-06-13 07:06:15 AM UTC | TRUE | Microsoft Windows Active Exploits, Rollins, ... |
| Oracle Java JRE 1.8.0 x64 | jre-8u321-windows-x64.exe | oracle | 72.2 MB | 2022-07-19 09:26:51 AM UTC | TRUE | Oracle Active Exploits |
| ubuntu | sudo 1.8.21-0ubuntu1.4 | todd_miller | 418.3 KB | 2022-06-18 01:54:58 PM UTC | FALSE | Baron Samedi |

Note: This value specifies the local date and time at which reboot will be mandated on all endpoints. Logged-in users can postpone reboot on their machines until this date-time value is reached. A prompt will appear on the user's screen before initiating a reboot.

- Remediation End Time

Remediation will be completed at the specified time

Create Patching Task

Task Controls

- Reboot Control
- Remediation End Time
- Patching Notification
- Remediation Scripts
- Test and Deploy

Task Name: Apply critical patches

Remediation Schedule: Immediate

Remediation End Time: 02:00 AM

Task Impact

- 1 Patch
- 1 Online
- 0 Offline

Assets and Patches Table

| Asset | Patch | Vendor | Size | Created | Status | Details |
|-------------------------------|---------------------------|-------------|----------|----------------------------|--------|---|
| Microsoft Windows 10 21H2 x64 | 2 patches | microsoft | 0 B | 2022-06-13 07:06:15 AM UTC | TRUE | Microsoft Windows Active Exploits, Rollins, ... |
| Oracle Java JRE 1.8.0 x64 | jre-8u321-windows-x64.exe | oracle | 72.2 MB | 2022-07-19 09:26:51 AM UTC | TRUE | Oracle Active Exploits |
| ubuntu | sudo 1.8.21-0ubuntu1.4 | todd_miller | 418.3 KB | 2022-06-18 01:54:58 PM UTC | FALSE | Baron Samedi |

- Patching Notification

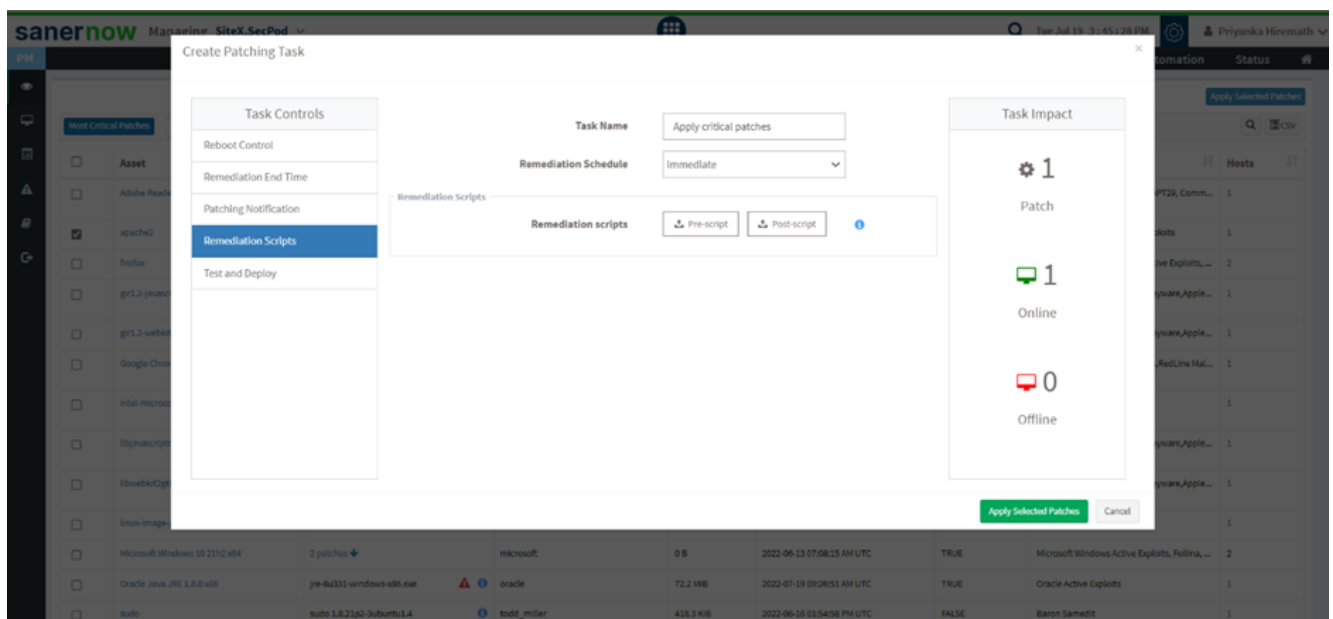
Give notification start message and notification end message so that you can be informed about the patching activity

The screenshot shows the 'Create Patching Task' dialog in the SanerNow interface. The dialog has a 'Task Controls' sidebar on the left with options like 'Reboot Control', 'Remediation End Time', 'Patching Notification' (selected), 'Remediation Scripts', and 'Test and Deploy'. The main area contains fields for 'Task Name' (Apply critical patches), 'Remediation Schedule' (Immediate), 'Notification Start Message' (System patching activity is schedul...), and 'Notification End Message' (System patching activity is complet...). A 'Task Impact' summary on the right shows 1 Patch, 1 Online, and 0 Offline. At the bottom right are 'Apply Selected Patches' and 'Cancel' buttons. The background shows a table of assets and patches.

| Asset | Patch | Vendor | Size | Last Patched | Status | Notes |
|-------------------------------|---------------------------|-------------|----------|----------------------------|--------|--|
| Microsoft Windows 10 21H2 x64 | 2 patches | microsoft | 0 B | 2022-06-13 07:06:15 AM UTC | TRUE | Microsoft Windows Active Exploits, Rollin... |
| Oracle Java JRE 1.8.0_305 | pre-8u321-windows-x86.exe | oracle | 72.2 MB | 2022-07-19 09:26:51 AM UTC | TRUE | Oracle Active Exploits |
| sudo | sudo 1.8.21a2-ubuntu1.4 | todd_miller | 418.3 KB | 2022-06-16 01:54:58 PM UTC | FALSE | Baron Samedi |

- Remediation Scripts

You can upload pre-remediation scripts and post-remediation scripts in the given file formats



Supported file formats in a script:

Windows: inf, reg, ps1, bat, exe, msi, msp

Linux: sh, deb, rpm

macOS: sh, pkg, dmg (pkg, app)

9. Click on **Apply Selected Patches**.

Click here to learn how to test and deploy patches in SanerNow: [How to apply missing patches in SanerNow? – SecPod – Documentation](#)

You have successfully created a task to test and deploy critical patches.