Protecting Against "WannaCry" Using Saner Solution

secpod

Introduction

In the last few days, we saw how "WannaCry" ransomware crippled 3 million Windows systems around 150 countries. Read WannaCry Ransomware: Digital example of a perfect storm to know technical details on "WannaCry".

In this article, we will cover step by step procedure to protect against "WannaCry" ransomware using Saner Solution.

"WannaCry" Infection Method

Before we jump to a solution, we need to understand the infection method to protect against "WannaCry". "WannaCry" make use of "**EternalBlue**" exploit, which is one of the exploits leaked to the public in mid of April 2017 by a group called the **Shadow Brokers**. "**WannaCry**" exploits a vulnerability in **Server Message Block 1.0 (SMBv1) protocol** (the issue is in the way that the SMBv1 server handles certain requests) and gains the ability to **execute code** on the target system. To exploit this vulnerability authentication is not required.

CVE-2017-0144 CVE identifier is assigned to this vulnerability.

In response to **Shadow Brokers** action, Microsoft released several patches addressing several vulnerabilities.

Code Name	Solution
"**EternalBlue**"	Addressed by MS17-010
"**EmeraldThread**"	Addressed by MS10-061
"**EternalChampion**"	Addressed by CVE-2017-0146 & CVE-2017-0147
"**ErraticGopher**"	Addressed prior to the release of Windows Vista
"**EsikmoRoll**"	Addressed by MS14-068
"**EternalRomance**"	Addressed by MS17-010
"**EducatedScholar**"	Addressed by MS09-050
"**EternalSynergy**"	Addressed by MS17-010
"**EclipsedWing**"	Addressed by MS08-067

Source: blogs.technet.microsoft.com

As we can see, in the above image, vulnerability (CVE-2017-0144) used by "**EternalBlue**" has been addressed by Microsoft in MS17-010 patch. This patch also addresses following CVE-2017-0143, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147 and CVE-2017-0148 additional vulnerabilities.

How to protect against "WannaCry"

There are two methods to protect against "WannaCry" ransomware,

1. **Solution**: Patch the vulnerability by applying MS17-010 - KB4012212 (**Recommended**)
2. **Workaround**: Disable SMBv1

In the following section, we will demonstrate how easy it is to use "**Saner Solution**" to protect against "**WannaCry**" by applying the patch or workaround to a group of devices in a network.

Protecting against "WannaCry" using Saner Solution

For illustration, we have chosen "**Windows 7**" system as it has the highest number of users presently.

How to check if a system is affected by the CVE-2017-0144 vulnerability?

Step 1: Log into Saner Solution dashboard.
Click "**Manage**" section on the left tab.
Click the "**Host Name**" link to see a particular system information (Figure 1).

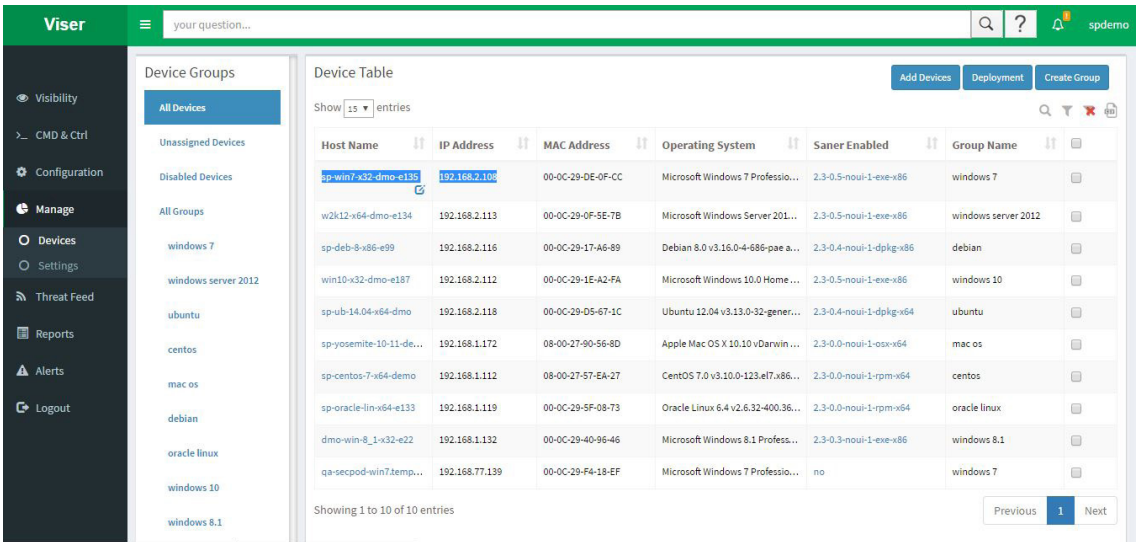

Fig 1

Step 2: Figure 2 shows "**sp-win7-x32-dmo-3135**" system information as it appears in Saner Solution. This system is used to demonstrate how to protect from "**WannaCry**" by fixing the CVE-2017-0144 vulnerability.

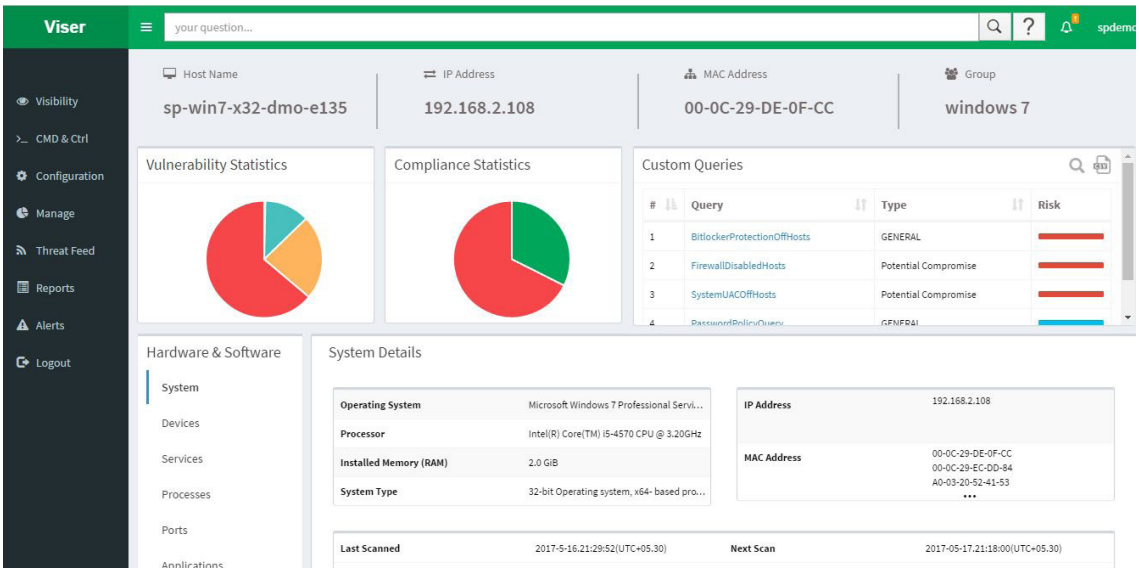

Fig 2

Step 3: Click "**Vulnerabilities**" section in the system information page. We can see the following vulnerability CVE-2017-0144 has been reported (Figure 3), which is being exploited by "**WannaCry**" to enter the system.

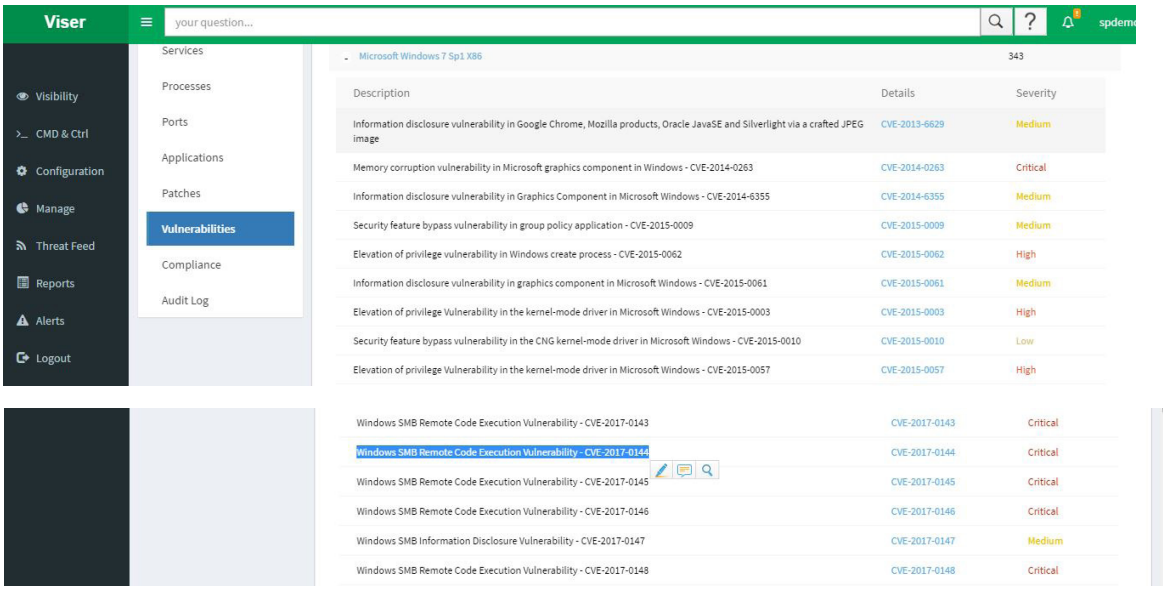

Fig 3

Step 4: Click "**Patches**" (Figure 4).
Click "**Missing Patches**" tab.
We can see the following patch KB4012212 needs to be installed to protect from "**WannaCry**".

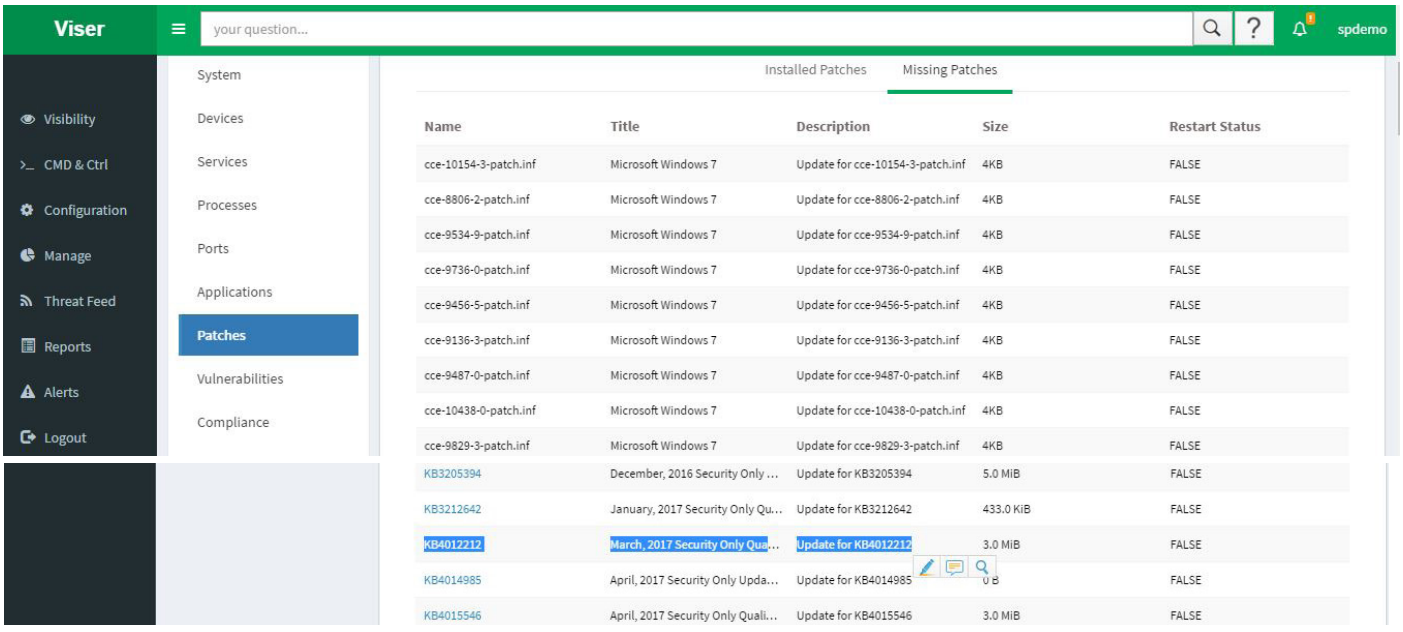

Fig 4

How to remediate CVE-2017-0144 vulnerability using Saner Solution?

Step 1: Click "**CMD & Ctrl**" section on the left tab.
Click "**Create Command**" (Figure 5).

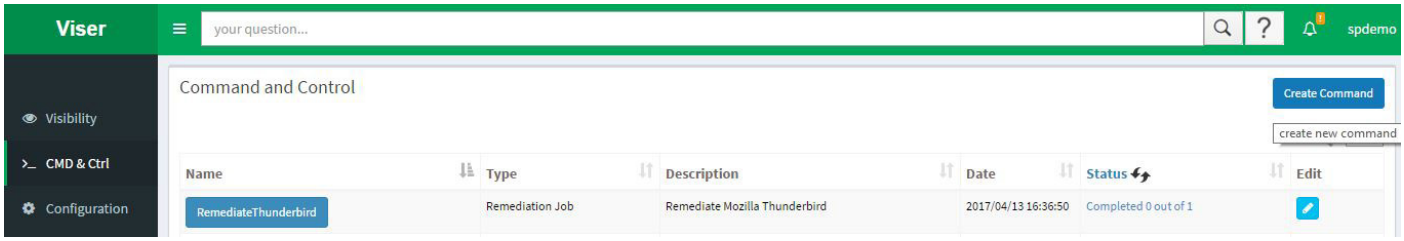

Fig 5

Step 2: Click "**Remediation**" icon as shown in figure 6.

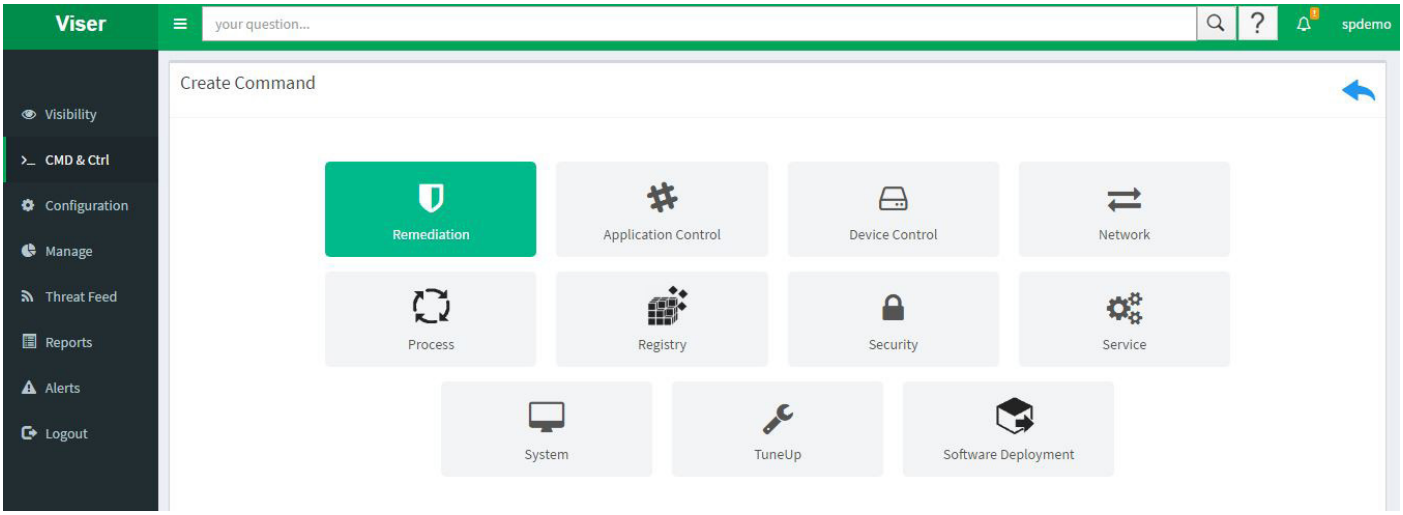

Fig 6

Step 3: Select "**Remediation Job**" from the drop-down list as shown in figure 7.

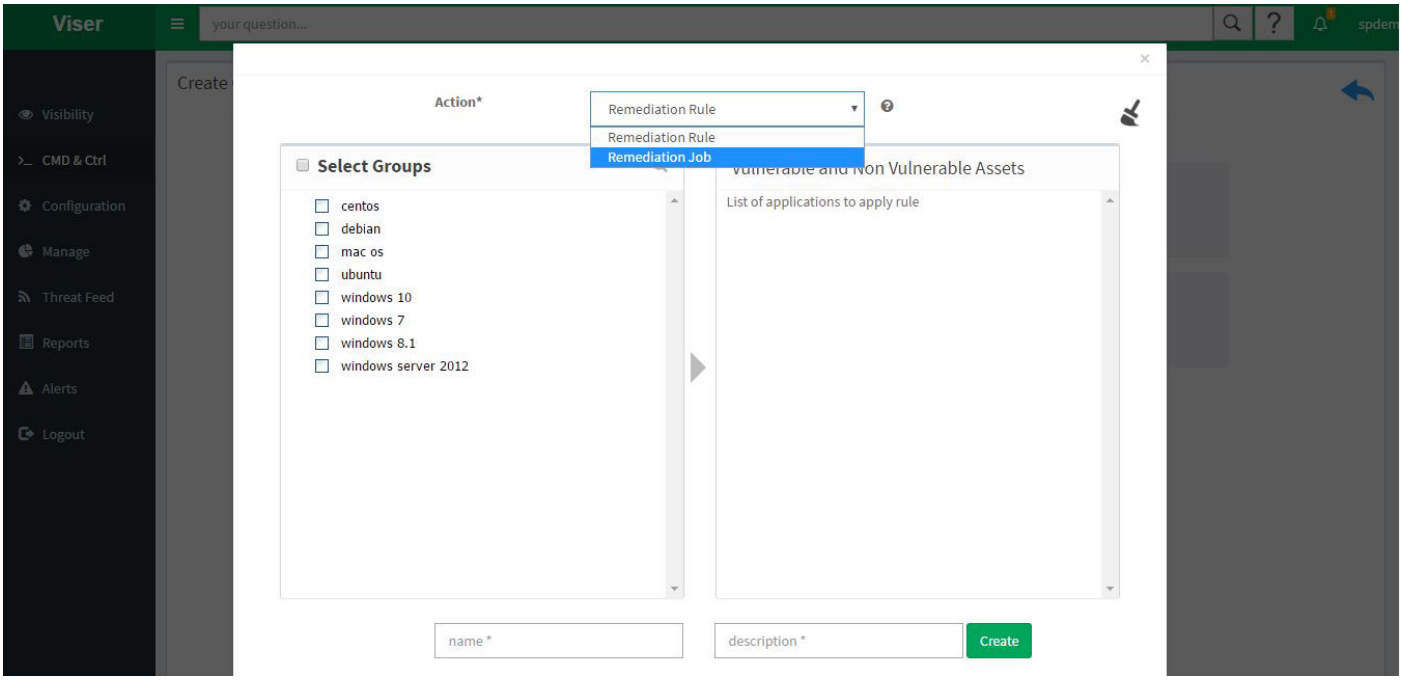

Fig 7

Step 4: Select all the "**groups**" or a specific "**device**" inside the group for which the patch needs to be applied. For example, "**sp-win7-x32-dmo-e135**" device under "**Windows 7**" group.
Click the arrow button in the middle. It will display a message "**click to see patches and devices**" to view patches and devices (Figure 8).

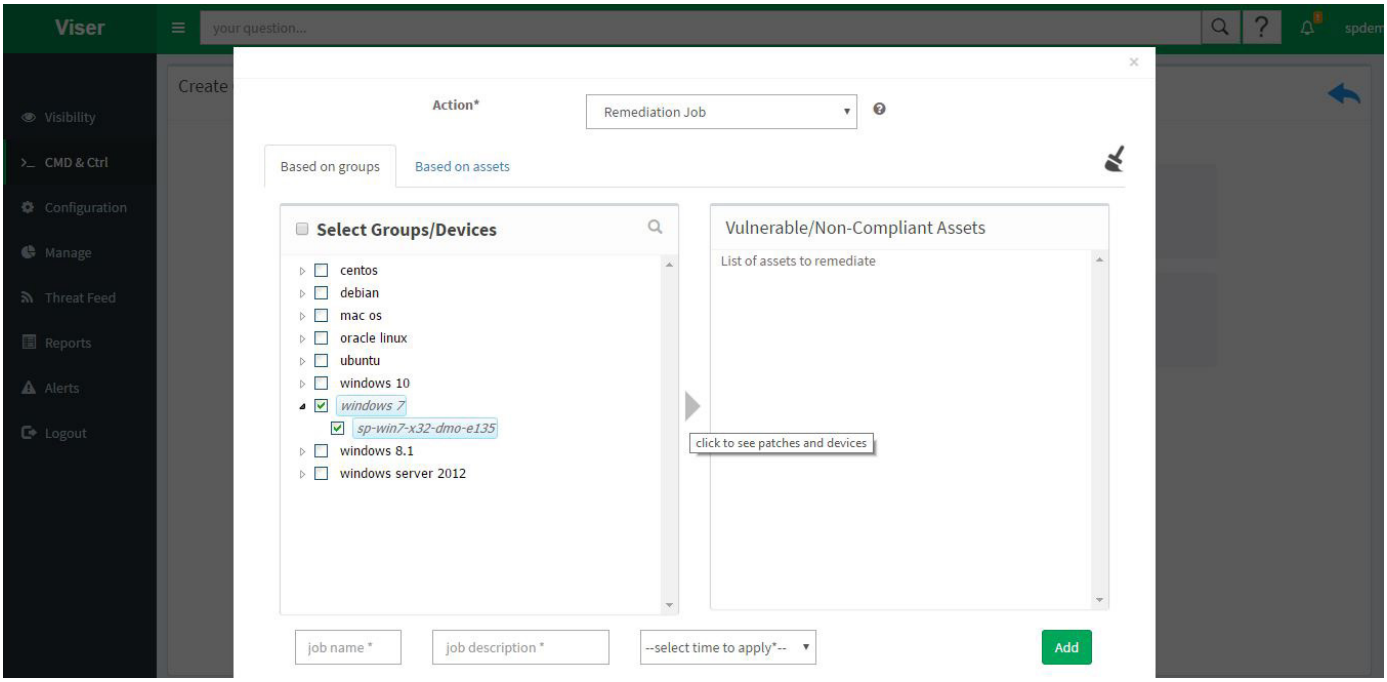

Fig 8

Step 5: Select patch "**Microsoft Windows**" -> "**Vendor Upgrade**" for a specific Windows you want to patch. For example, select "**Microsoft Windows 7 sp1 x86**" -> "**Vendor upgrade**" as shown figure 9.

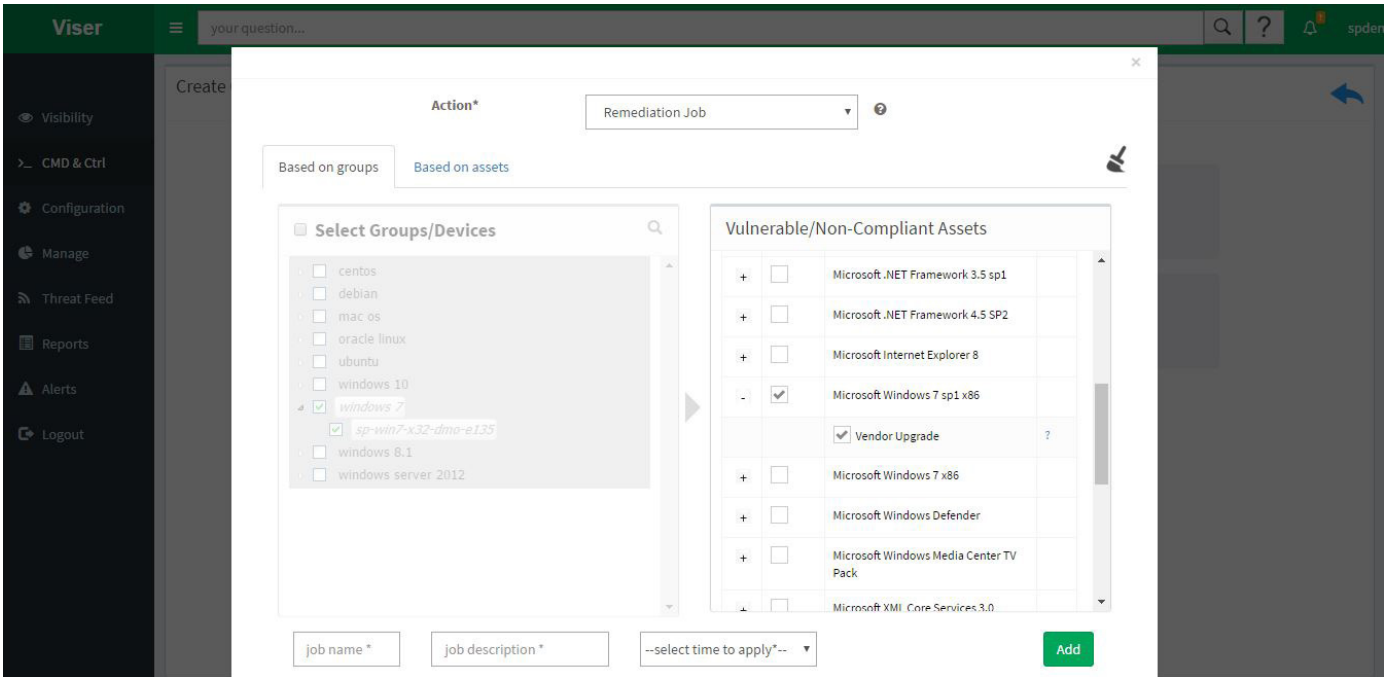

Fig 9

Step 6 (Optional): Click "?" next to "**Vendor Upgrade**" to see the patches included. For example, we need to apply "KB4012212" which is included in the "**Microsoft Windows 7 sp1 x86**" patch, as shown in figure 10.

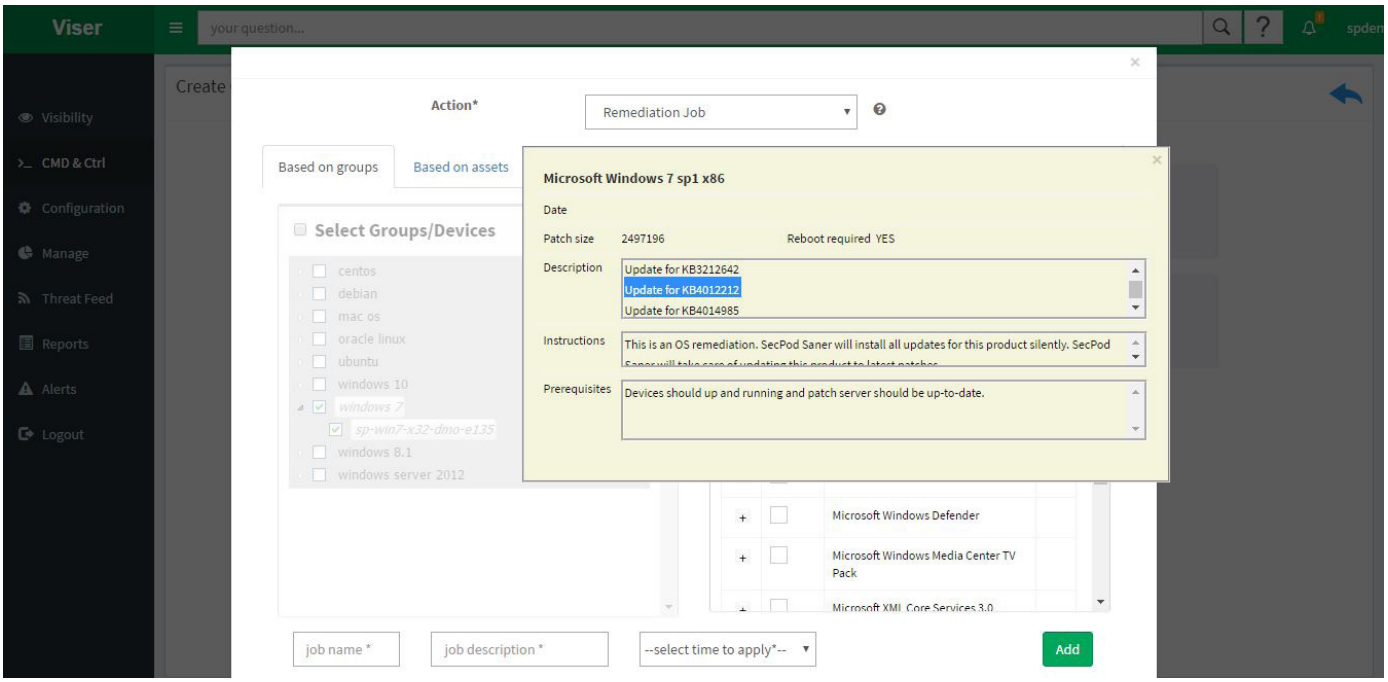

Fig 10

Step 7: Select "**select time to apply**" from the drop-down list. The patch can be applied **immediately**, **after a scheduled scan** or at a **custom** time.
Enter "**Job name**" and "**Job Description**" in the text box. For example, here the job name is "**WannaCryPatchRemJob**" as shown in figure 11.

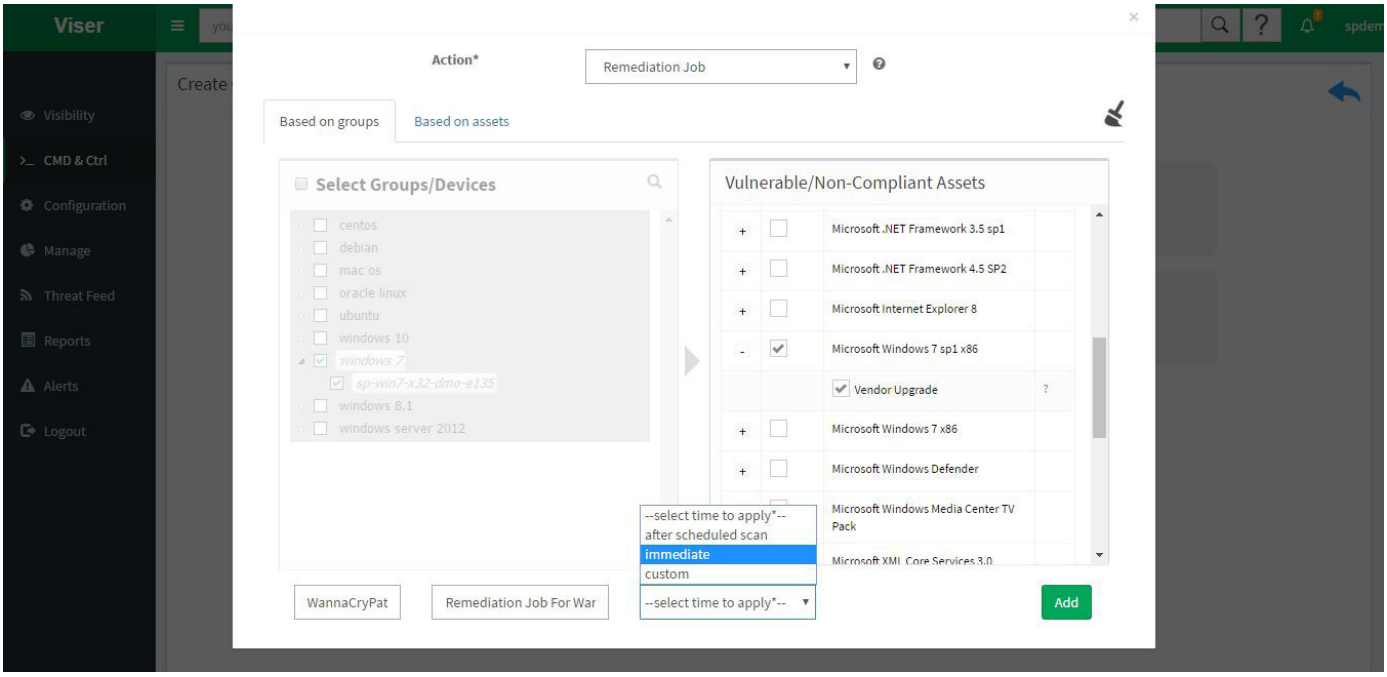

Fig 11

Step 8: Click "**Add**" button to create "**Remediation Job**", as shown in figure 12.

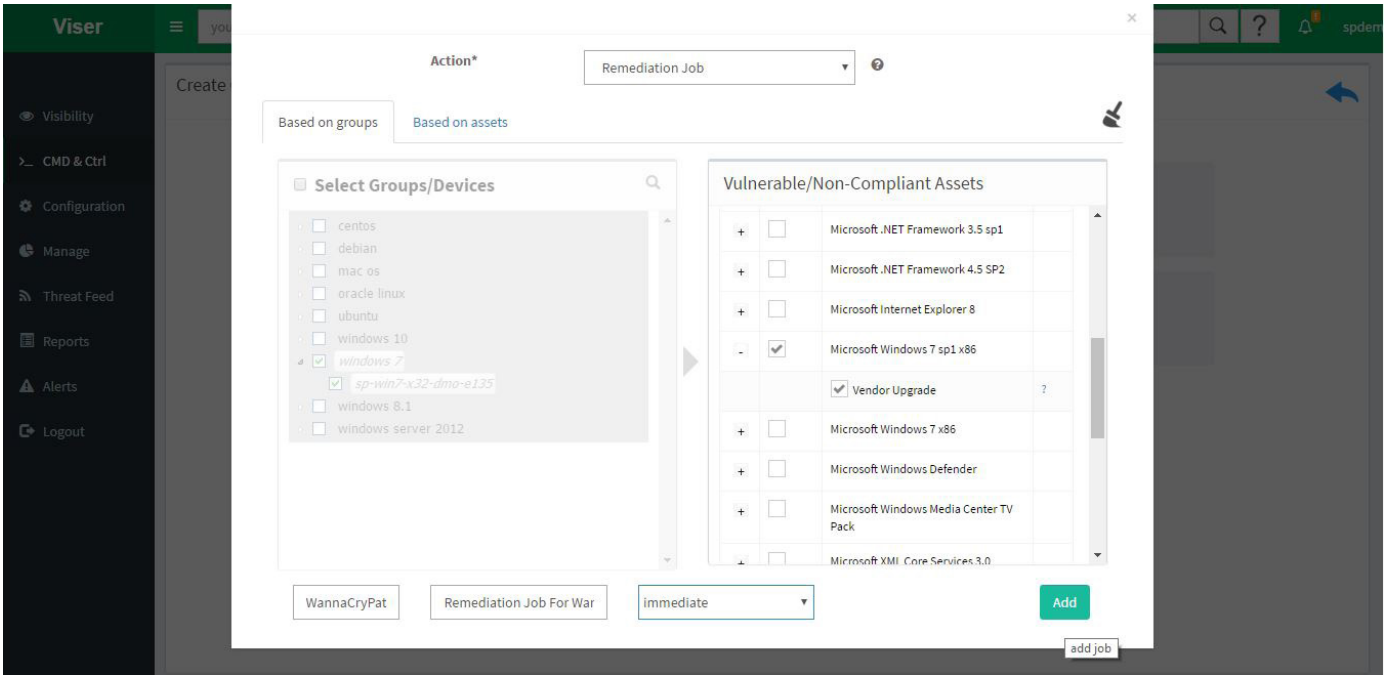

Fig 12

Step 9: Remediation job with "**WannaCryPatchRemJob**" name is created successfully, as shown in figure 13.

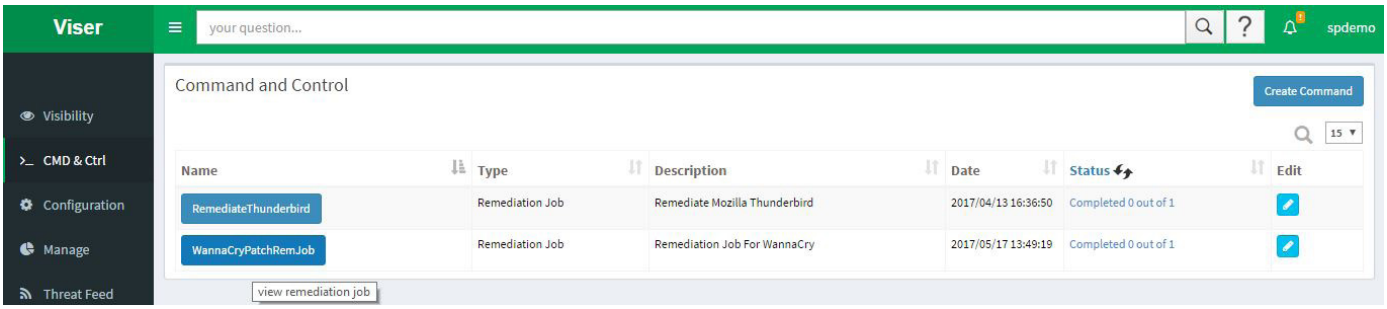

Fig 13

Step 10 (Optional): To see the status of the remediation job click on status, for example, "**Completed 0 out of 1**" as shown in figure 14.

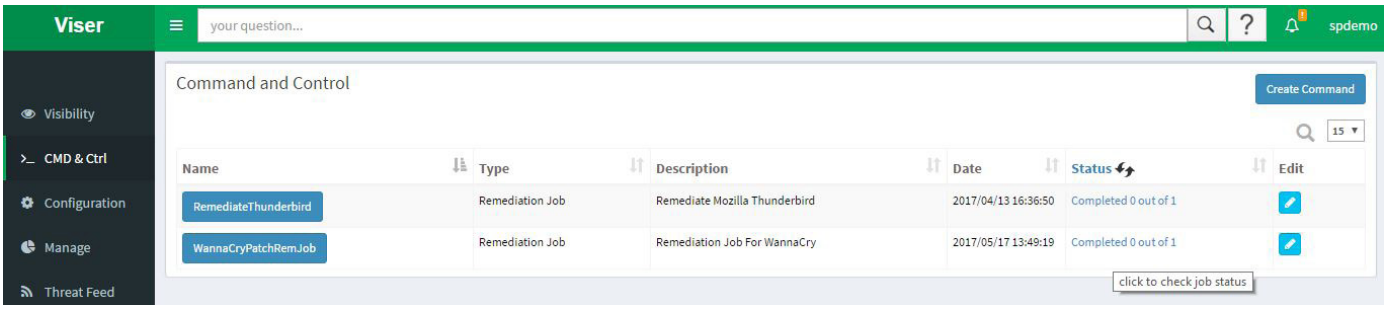

Fig 14

Step 11 (Optional): Remediation status shows overall status as "**ongoing**" and specific patch as "**queue**" (Figure 15).

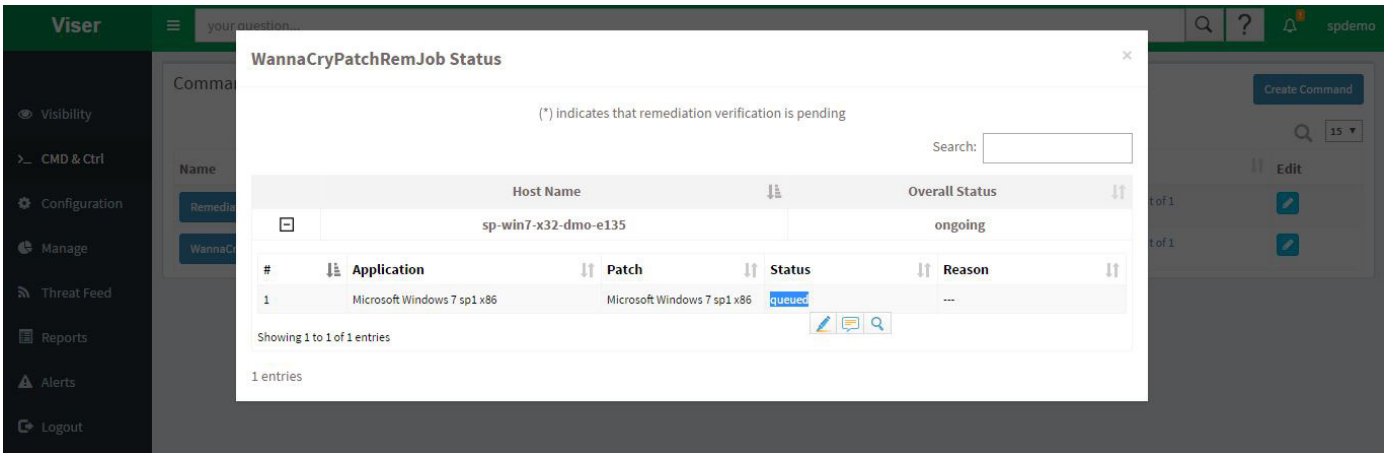

Fig 15

Step 12: Successful remediation requires a reboot. If the overall remediation job status says "**reboot needed**" (Figure 16), then reboot the systems to continue the remediation process.

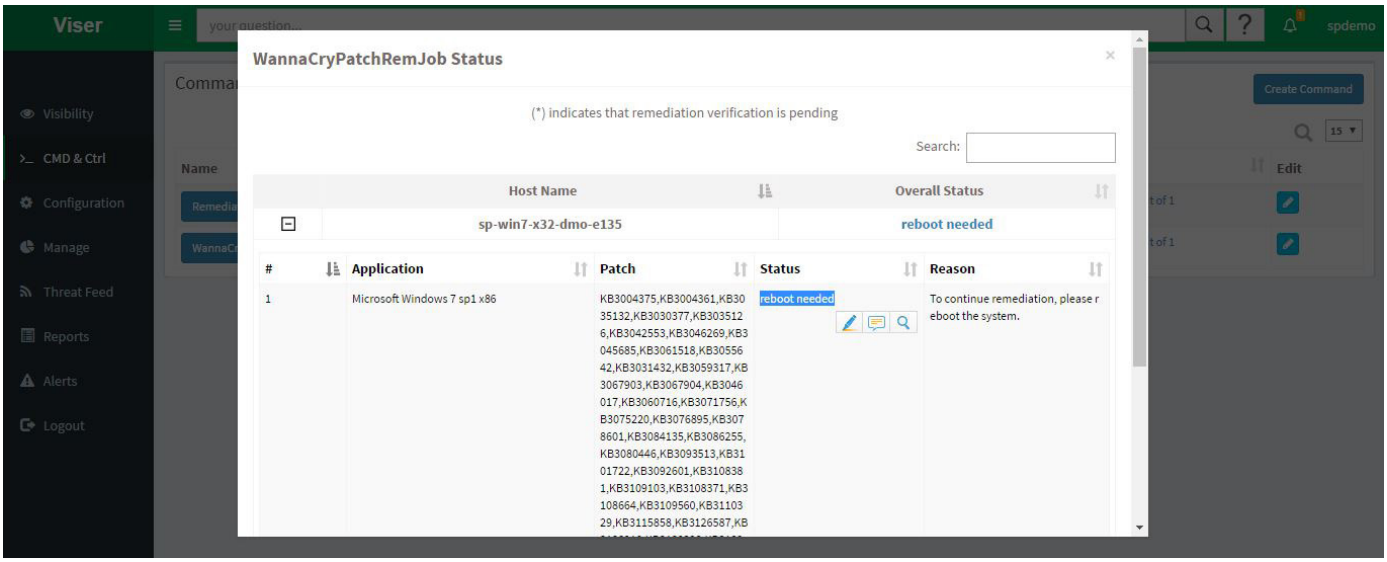

Fig 16

Step 13: Once the remediation job is successful, the overall status changes to "**success**" (Figure 17).

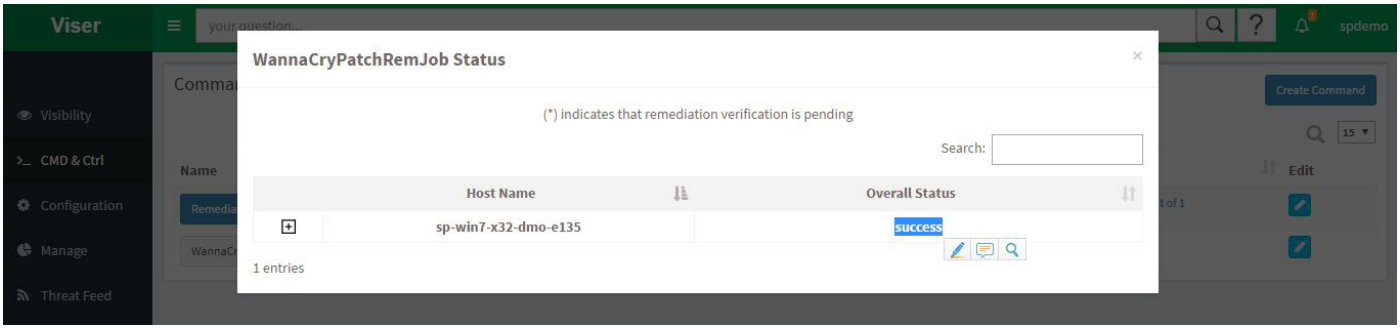

Fig 17

Step 14: To verify "CVE-2017-0144" vulnerability is fixed or not follow step 3. Search "CVE-2017-0144". It should not be listed in the Vulnerability section.

About Us

SecPod Technologies creates cutting edge products to ensure endpoint security. SecPod's deep information security expertise exceptionally positions the company to help solve complex endpoint security challenges. Headquartered in Bangalore with operations in USA, SecPod's products are deployed across diversified verticals.

Contact Us

Web: www.secpod.com Tel: +91-80-4121 4020
Email: info@secpod.com +1-918-625-3023