Protecting Against "WannaCry" Using Saner Solution

RIDIO 64

box sha

secpod

1011011011011

86 1.201 1

ton

ZF KINON

undex

Introduction

In the last few days, we saw how "WannaCry" ransomware crippled 3 million Windows systems around 150 countries. Read <u>WannaCry Ransomware: Digital example of a perfect storm</u> 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 (<u>CVE-2017-0144</u>) used by "**EternalBlue**" has been addressed by Microsoft in <u>MS17-010</u> patch. This patch also addresses following <u>CVE-2017-0143</u>, <u>CVE-2017-0145</u>, <u>CVE-2017-0145</u>, <u>CVE-2017-0145</u>, <u>CVE-2017-0148</u> additional vulnerabilities.

How to protect against "WannaCry"

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

- 1. Solution: Patch the vulnerability by applying <u>MS17-010</u> 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).

• Visibility • Visibility • CMD & Ctrl Device Groups Device Table Device Table Show [3 v = ntriles Device Table Show [3 v = ntriles Shohow [3 v = ntriles Show [3 v = ntriles	spueme
• Visibility All Devices All Devices Show 15 • entries • • • • • • • • • • • • • • • • • • •	roup
> CMD & Ctrl Unassigned Devices Host Name IP Address MAC Address Operating System Saner Enabled Group Name III © Configuration Disabled Devices Big_win7/3524me-113 Big2.662.102 ObcC29-DE-DF-CC Microsoft Windows TProfession 2-3-0-5-noul-1-exe+366 windows 7 Imade: Since	x 📾
• Configuration • Disabled Devices • Manage All Groups • All Groups • Manage All Groups • Manage • Manage	
C Manage All Groups w2k12x64-dmo-e134 192.168.2.113 00-0C290-F5E-78 Microsoft Windows Server 201. 23-0.5-noul-1-dpkg.x64 windows server 2012 windows server 2012 windows server 2012 windows server 2012 192.168.2.113 00-0C290-F5E-78 Microsoft Windows Server 201. 23-0.5-noul-1-dpkg.x64 debian odd S Strings windows server 2012 windows server 2012 192.168.2.113 00-0C290-IFA-68 Debian 8.0 v3.16.0-4-686-pae. 23-0.4-noul-1-dpkg.x64 debian	
O Devices windows 7 sp-deb-8x86-e99 192.168.2.116 00-0C29-17x6-89 Debias 8.0v3.16.0-4685-pae.a. 2.3-0.4-noui-1-dpkgx86 debian S Settings windows server 2012 windows 32-dmo-e187 192.168.2.112 00-0C29-1Ex42FA Microsoft Windows 10.0.0 Home 2.3-0.4-noui-1-dpkgx86 windows 10 iminows 10	
windows server 2012 windows server 2012 windows 32-dmo-e187 192.168.2.112 00-0C29-1E-k2-FA Microsoft Windows 10.0 Home 2.3-0.5-noui-1-exe-x86 windows 10 ubuntu sp-ub-14.04+x64-dmo 192.168.2.118 00-0C29-05-67-1C Ubuntu 12.04/x3.13.0-32-gener 2.3-0.4-noui-1-dpkgx64 ubuntu	
ubuntu ubuntu sp-ub-14.04.x64-dmo 192.168.2.118 00-0C-29-D5-67-1C Ubuntu 12.04.v3.13.0-32.gener 2.3-0.4-noui-1.dplg.x64 ubuntu	0
centos sp-yosemite-10-11-de 192.168.1.172 08-00-27-90-56-8D Apple Mac OS X 10.10 vDarwin 2.3-0.0-noui-1-ooxx64 mac os	0
A Alerts mac os sp-centos:7x64-demo 192.168.1.112 08-00-27-57-EA-27 CentOS 7.0 v3.10.0-123.el7.x86 2.3-0.0-noui-1-rpm-v64 centos	(
Ce Logout debian sp-oracle-linx64-e133 192.168.1.119 00-0C29-5F-08-73 0racle Linux 6.4 v2.6.32-400.36 2.3-0.0-noui-1-rpm:v64 oracle linux	0
dmo-win-8_1x32-e22 192.168.1.132 00-0C2940-96-46 Microsoft Windows 8.1 Profess 2.3-0.3-noui-1-exe-x86 windows 8.1	
ga-secpod-win7.temp 192.168.77.139 00-0C-29-F4-18-EF Microsoft Windows 7 Professio no windows 7	0
windows 8.1 Previous 1	Next

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 <u>CVE-2017-0144</u> vulnerability.







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

Viser	≡ your question			Q ? 🔎 spderr
	Services	Microsoft Windows 7 Sp1 X86		343
Visibility	Processes	Description	Details	Severity
>_ CMD & Ctrl	Ports	Information disclosure vulnerability in Google Chrome, Mozilla products, Oracle JavaSE and Silverlight via a crafted JPEG image	CVE-2013-6629	Medium
Configuration	Applications	Memory corruption vulnerability in Microsoft graphics component in Windows - CVE-2014-0263	CVE-2014-0263	Critical
🊱 Manage	Patches	Information disclosure vulnerability in Graphics Component in Microsoft Windows - CVE-2014-6355	CVE-2014-6355	Medium
- manage	Vulnerabilities	Security feature bypass vulnerability in group policy application - CVE-2015-0009	CVE-2015-0009	Medium
እ Threat Feed	Compliance	Elevation of privilege vulnerability in Windows create process - CVE-2015-0062	CVE-2015-0062	High
🗐 Reports		Information disclosure vulnerability in graphics component in Microsoft Windows - CVE-2015-0061	CVE-2015-0061	Medium
A Alerts	Audit Log	Elevation of privilege Vulnerability in the kernel-mode driver in Microsoft Windows - CVE-2015-0003	CVE-2015-0003	High
		Security feature bypass vulnerability in the CNG kernel-mode driver in Microsoft Windows - CVE-2015-0010	CVE-2015-0010	Low
C• Logout		Elevation of privilege Vulnerability in the kernel-mode driver in Microsoft Windows - CVE-2015-0057	CVE-2015-0057	High
		Windows SMB Remote Code Execution Vulnerability - CVE-2017-0143	CVE-2017-0143	Critical
		Windows SMB Remote Code Execution Vulnerability - CVE-2017-0144	CVE-2017-0144	Critical
		Windows SMB Remote Code Execution Vulnerability - CVE-2017-0145	CVE-2017-0145	Critical
		Windows SMB Remote Code Execution Vulnerability - CVE-2017-0146	CVE-2017-0146	Critical
		Windows SMB Information Disclosure Vulnerability - CVE-2017-0147	CVE-2017-0147	Medium
		Windows SMB Remote Code Execution Vulnerability - CVE-2017-0148	CVE-2017-0148	Critical

Fig 3

Step 4: Click "Patches" (Figure 4).

Click "Missing Patches" tab.

We can see the following patch <u>KB4012212</u> needs to be installed to protect from "WannaCry".

Viser						Q ? Q spde
	System		Inst	talled Patches Missing Pat	ches	
Visibility	Devices	Name	Title	Description	Size	Restart Status
> CMD & Ctrl	Services	cce-10154-3-patch.inf	Microsoft Windows 7	Update for cce-10154-3-patch.inf	4KB	FALSE
Configuration	Processes	cce-8806-2-patch.inf	Microsoft Windows 7	Update for cce-8806-2-patch.inf	4KB	FALSE
A	Ports	cce-9534-9-patch.inf	Microsoft Windows 7	Update for cce-9534-9-patch.inf	4KB	FALSE
🖙 Manage		cce-9736-0-patch.inf	Microsoft Windows 7	Update for cce-9736-0-patch.inf	4KB	FALSE
Threat Feed	Applications	cce-9456-5-patch.inf	Microsoft Windows 7	Update for cce-9456-5-patch.inf	4KB	FALSE
Reports	Patches	cce-9136-3-patch.inf	Microsoft Windows 7	Update for cce-9136-3-patch.inf	4KB	FALSE
A Alarta	Vulnerabilities	cce-9487-0-patch.inf	Microsoft Windows 7	Update for cce-9487-0-patch.inf	4KB	FALSE
Alerts	Compliance	cce-10438-0-patch.inf	Microsoft Windows 7	Update for cce-10438-0-patch.inf	4KB	FALSE
🕒 Logout		cce-9829-3-patch.inf	Microsoft Windows 7	Update for cce-9829-3-patch.inf	4KB	FALSE
		KB3205394	December, 2016 Security Only	Update for KB3205394	5.0 MiB	FALSE
		KB3212642	January, 2017 Security Only Qu	Update for KB3212642	433.0 KiB	FALSE
		KB4012212	March, 2017 Security Only Qua	Update for KB4012212	3.0 MIB	FALSE
		KB4014985	April, 2017 Security Only Upda	Update for KB4014985	Q B	FALSE
		KB4015546	April, 2017 Security Only Quali	Update for KB4015546	3.0 MiB	FALSE





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).

Viser	your question							Q ?	Δ.	spdemo
	Command and Control								Create Cor	mmand
Visibility									create new	command
>_ CMD & Ctrl	Name	11	Туре	41	Description 11	Date 11	Status 4		lî Edit	
Configuration	RemediateThunderbird		Remediation Job		Remediate Mozilla Thunderbird	2017/04/13 16:36:50	Completed 0 out of 1			
					Fig 5					

Viser Q ? your question.. Create Command Visibility >__ CMD & Ctrl U # 1 Configuration Application Control Device Control Network 🚱 Manage Threat Feed 0 ø 0. Reports Security Service Process Registry A Alerts JC. C Logout Software Deployment System TuneUp Fig 6

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

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

Viser	yourquesti	on				E.	Q ? A spden
Visibility	Create	Action*	Remediation Rule	•	0	Ł	*
>_ CMD & Ctrl		Select Groups	Remediation Job	vuinerable and h	on Vulnerable Assets		
Configuration		centosdebian	*	List of applications to	apply rule	*	
🚯 Manage		mac os					
♣ Threat Feed		windows 10					
Reports		windows \$7					
Alerts							
🕒 Logout							
		name*		description *	Create		

Fig 7

secrod

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).

Viser	Jour question	Q ? 🖓 spder
 Visibility CMD & Ctrl 	Create Action* Remediation Job Based on groups Based on assets	*
 Configuration Manage 	Select Groups/Devices Q Vulnerable/Non-Compliant Assets List of assets to remediate *	
ন্স Threat Feed	Image: book of the second s	
▲ Alerts	 ▶ in windows 10 ▶ in windows 7 ▶ in windows 8.1 ▶ in windows server 2012 	
	job name * job description *select time to apply* • • Add	

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.

Visibility	Action*	Remediation Job			v 😧			
CMD & Ctrl	Based on groups Based on assets						2	
Configuration	Select Groups/Devices	Q	Vulr	erable/	/Non-Compliant Assets			
Manage			+		Microsoft .NET Framework 3.5 sp1		-	
Threat Feed			+		Microsoft .NET Framework 4.5 SP2			
Reports			+		Microsoft Internet Explorer 8			
Alerts			1.3	~	Microsoft Windows 7 sp1 x86		1.1	
Logout	 ✓ windows 7 ✓ sp-win7-x32-dmo-e135 				Vendor Upgrade	?		
			+		Microsoft Windows 7 x86			
			+		Microsoft Windows Defender			
			+		Microsoft Windows Media Center TV Pack			
					Carlor and Approximation of the state			





Viser	≡ your q	uestion								Q ?	
 Visibility 	Create		Action*	R	emediation Job			v Ø	×		+
>_ CMD & Ctrl		Based on groups	Based on assets	Microsoft V	Vindows 7 sp1 x	86			×		
Configuration		Select Gro	ouns/Devices	Date							
🕒 Manage			subs/berrees	Patch size Description	2497196 Update for KB32	12642	Rebo	ot required YES	*		
局 Threat Feed					Update for KB40 Update for KB40	12212 14985			•		
Reports				Instructions	This is an OS rem	ediation.	SecPod Sa	ner will install all updates for this product si	lently. SecPod		
Alerts		windows		Prerequisites	Devices should u	p and rur	ning and p	atch server should be up-to-date.	*		
C Logout									* :		
						+	6	Microsoft Windows Defender			
						+		Microsoft Windows Media Center TV Pack			
					-	1		Microsoft XMI Core Services 3.0			
		job name *	job descriptio	on*	select tim	ie to app	oly* ▼		Add		
					Fig 1	0					

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.

Viser	Jan you								×	Q ? 4
	Create		Action*	Remediation Job			• Ø			
		Based on groups	Based on assets						*	
		Select Gr	ouns/Devices		Vulr	erable/	Non-Compliant As	sets		
		- Select on	546575657665							
					+		Microsoft .NET Framewo	rk 3.5 sp1		
					+		Microsoft .NET Framewo	rk 4.5 SP2		
					+		Microsoft Internet Explor	rer 8		
						~	Microsoft Windows 7 sp1	. x86	111	
		a ♥ windows ♥ sp-windows		P			Vendor Upgrade	?		
					+		Microsoft Windows 7 x86	6		
					+		Microsoft Windows Defe	nder		
			select tin after schee	time to apply* heduled scan		Microsoft Windows Medi Pack	a Center TV			
					2		Microsoft XMI Core Serv	ices 3.0	•	
		WannaCryPat	Remediation Job For Wa	arselect tin	ne to an	olv* ▼			dd.	
		wannaciyrat	Remeatation Job Por Wa	"select till	ine to ap	ny ,				

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.

Viser	your question							Q	? 4	spdemo
Visibility	Command and Control								Create Co	mmand
>_ CMD & Ctrl	Name	ĻŁ	Туре	Description	-11	Date 11	Status 49		LÎ Edit	
Configuration	RemediateThunderbird		Remediation Job	Remediate Mozilla Thunderbird		2017/04/13 16:36:50	Completed 0 out of 1			
🚱 Manage	WannaCryPatchRemJob		Remediation Job	Remediation Job For WannaCry		2017/05/17 13:49:19	Completed 0 out of 1			
♣ Threat Feed	view remediation job	[
				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.

Viser	your question						Q ?	<u>ک</u>	spdemo
	Command and Control							Create Co	mmand
👁 Visibility								Q	15 🔻
>_ CMD & Ctrl	Name	1h	Type 👫	Description	Date 11	Status 4		↓† Edit	
Configuration	RemediateThunderbird		Remediation Job	Remediate Mozilla Thunderbird	2017/04/13 16:36:50	Completed 0 out of 1			
🚱 Manage	WannaCryPatchRemJob		Remediation Job	Remediation Job For WannaCry	2017/05/17 13:49:19	Completed 0 out of 1			
🔊 Threat Feed						click to check	job status	1	





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

Viser	your question						Q ? A spdemo
	Wanna	×	Control or second				
Visibility			Create Command				
>_ CMD & Ctrl	Name				Search:		II Edit
Configuration	Remedia	Hos	it Name	11	Overall Status	↓† t of 1	
🕒 Manage	WannaCr	sp-win7	x32-dmo-e135		ongoing	tofl	
ন Threat Feed	#	Application Microsoft Windows 7 sp1 x86	JT Patch Microsoft Window	ws 7 sp1 x86 queued	↓↑ Reason 	11	
Reports	Showing 1						
🛕 Alerts	1 entries						
🕒 Logout							

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.

Viser	= your a	uestion								Q	spdemo
	Comma	WannaCry	/PatchRemJob Status						×		Create Command
Visibility				(*) indicate	es that remediation verifica	ition is pendir	ng	enu			Q 15 T
>_ CMD & Ctrl	Name						9	Search:			LT Edit
Configuration	Remedia			Host Name		11	Ove	rall Status	11	t of 1	
🕼 Manage	WannaCr		sp-w	in7-x32-dmo-	e135	1	reb	oot needed		t of 1	
⋒ Threat Feed		1	Application Microsoft Windows 7 sp1 x86	11	Patch [] KB3004375,KB3004361,KB30	Status reboot neede	T.	Reason To continue remedi	4T ation, please r		
Reports					35132,KB3030377,KB303512 6,KB3042553,KB3046269,KB3 045685 KB3061518 KB30556		2 🖻 9	eboot the system.			
🛦 Alerts					42,KB3031432,KB3059317,KB 3067903,KB3067904,KB3046						
🕞 Logout					01, M3001100, M3001100, M30 8007520, KB3076895, KB307 8601, KB3084135, KB308255, KB3082646, KB3093513, KB3 1, KB3109103, KB3108371, KB3 108664, KB3109560, KB3103 29, KB3115858, KB3126587, KB					•	

Fig 16

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

Viser		auestion					Q	? 🖓 spo	
	Comma	WannaCryPatchRemJob Status ×						(Compared and	
Visibility	550000		(*) indicate	s that remediation verifica	tion is pending			Q 15	•
>_ CMD & Ctrl	Name				Search:			41 Edit	
Configuration	Remedia		Host Name	11	Overall Status	41			
		+	sp-win7-x32-dmo-e135		success				
🚱 Manage	WannaCr	1 entries			2 🖻 Q				
🔊 Threat Feed									

Fig 17

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

Protecting Against "WannaCry" Using Saner Solution

secrod

26Cb00

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

