CBS Total Technology

Date published: May 18, 2017

Actions Required to Protect Microsoft Machines from WannaCry Ransomware Attacks

Following the WannaCry (aka WannaCrypt) Ransomware Attacks, Microsoft released an announcement outlining which Microsoft customers are vulnerable and how they can protect themselves from these attacks.

The following is an excerpt from Microsoft's post:

- In March, we released a security update which addresses the vulnerability that these attacks are exploiting. Those who have Windows Update enabled are protected against attacks on this vulnerability. For those organizations who have not yet applied the security update, we suggest you immediately deploy Microsoft Security Bulletin MS17-010.

- For customers using Windows Defender, we released an update earlier today which detects this threat as Ransom:Win32/WannaCrypt. As an additional "defense-in-depth" measure, keep up-to-date anti-malware software installed on your machines. Customers running anti-malware software from any number of security companies can confirm with their provider, that they are protected.

- This attack type may evolve over time, so any additional defense-in-depth strategies will provide additional protections. (For example, to further protect against SMBv1 attacks, customers should consider blocking legacy protocols on their networks).

Read more >>

Webroot and Malwarebytes have also provided the following posts regarding the WannaCry attacks and their methodology to protect against them.

- **Webroot:** Second WannaCry wave spreads the globe
- **Malwarebytes:** WanaCrypt0r ransomware hits it big just before the weekend

Actions Required to Protect Microsoft Machines from WannaCry Ransomware Attacks

Which patches should I look for and where can I find them?

1) If your systems are up-to date with the March 2017 Security patch, your machines should be protected. Additionally, because of Microsoft's cumulative patch rollup model, if the April 2017 or May 2017 Security patches are installed, your machines should be protected as well.

2) To review whether the updates are installed or not, please refer to the Installed Update Report under

Reports → Patches → Microsoft Update Multi Site Report

and select all of your sites/systems. If you are looking for a specific patch, enter the desired KB article and click Submit. If not, just click Submit.

3) After submitting, the report will list all patches that are installed on each system. To view more details, click on the hyperlinked text, Against System or Patch. This report can be exported.

The table on the following page shows the required Microsoft Security Updates that have been released since March for each version of Windows OS. All patches listed in this table contain the security update that has been shown to protect against the WannaCry Ransomware Attacks. These patches have been whitelisted by Continuum.

CBS Total Technology

Date published: May 18, 2017

Windows Operating System	Mar-17	Apr-17		May-17		Related Microsoft Articles
	Patch Released	Supersedes Previous Patch? (Yes/No)	Patch Released	Supersedes Previous Patch? (Yes/No)	Patch Released	
Windows OS versions supported by Microsoft						
Vista	KB4012598	N/A	None	Yes	KB4018466	Windows SMB Vulnerability in Windows Server 2008: May 9, 2017
Server 2008	KB4012598	N/A	None	Yes	KB4018466	
7	KB4012215	Yes	KB4015549	Yes	KB4019264	May 2017 Monthly Rollup- Windows 7 and Windows- Server 2008 R2
Server 2008 R2	KB4012215	Yes	KB4015549	Yes	KB4019264	
8	KB4012217	Yes	KB4015551	Yes	KB4019216 KB4012598	May 2017 Monthly Rollup - Windows Server 2012
Server 2012	KB4012217	Yes	KB4015551	Yes	KB4019216 KB4012598	
8.1	KB4012216	Yes	KB4015550	Yes	KB4019215	March 2017 Monthly Rollup- Windows 8.1 and Windows Server 2012 R2
Server 2012 R2	KB4012216	Yes	KB4015550	Yes	KB4019215	
Windows OS versions that are no longer supported by Microsoft						
XP	None	N/A	None	TBD	KB4012598	--
Server 2003	None	N/A	None	TBD	KB4012598	--

Additional details:

Windows Vista Service Pack 2 & Windows Server 2008 for 32/64-bit Systems Service Pack 2 & Windows Server 2008 for 32/64-bit Systems Service Pack 2 (Server Core installation) (4012598)

- In March 2017, Microsoft released the patch SMB (MS17-010) KB4012216, which was Whitelisted by Continuum on March 29, 2017.
- In April 2017, no patches were released by Microsoft.
- In May 2017, Microsoft released KB4018466, which replaces the patch released in March.

More information can be found here: https://support.microsoft.com/en-us/help/4018466/title

Windows 7 for 32/64-bit Systems Service Pack 1 & Windows Server 2008 R2 for x64-based Systems Service Pack 1 (4012215)

- In March 2017, Microsoft released the patch SMB (MS17-010) KB4012215, which was Whitelisted by Continuum on March 29, 2017.
- In April 2017, Microsoft released KB4015549, which replaced the patch released in March.
- In May 2017, Microsoft released KB4019264, which replaces the patch released in April, and therefore also replaces the patch released in March.

More information can be found here: https://support.microsoft.com/en-us/help/4019264/windows-7-update-kb4019264

Windows 8 & Windows Server 2012 (4012217)

- In March 2017, Microsoft released the patch SMB (MS17-010) KB4012217, which was Whitelisted by Continuum on March 29, 2017.
- In April 2017, Microsoft released KB4015551, which replaced the patch released in March. In May 2017, Microsoft released KB4019216, which replaces the patch released in April, and therefore also replaces the patch released in March.

More information can be found here: https://support.microsoft.com/en-us/help/4019216

Windows 8.1 for 32/64-bit Systems & Windows Server 2012 R2 (4012216)

- In March 2017, Microsoft released the patch SMB (MS17-010) KB4012216, which was Whitelisted by Continuum on March 29, 2017.
- In April 2017, Microsoft released KB4015550, which replaced the patch released in March.
- In May 2017, Microsoft released KB4019215, which replaces the patch released in April, and therefore also replaces the patch released in March.

More information can be found here: https://support.microsoft.com/en-us/help/4012216/march-2017-security-monthly-quality-rollup-for-windows-8-1-and-windows-server-2012-r2

Windows XP & Windows Server 2003

Microsoft ended support for Windows XP and Windows Server 2003 in April 2014, but has released a critical security patch to protect against the WannaCry Ransomware Attacks in May 2017.

In May 2017, Microsoft released KB4012598 for Windows XP and Windows Server 2003. This patch had previously been included in the March rollup for supported Windows versions and has now been made available for Windows XP and Server 2003.

This patch has not been made available for these versions through the Windows Update website and therefore has not been auto-deployed on machines running Windows XP or Server 2003. Continuum will be making scripts available Friday, May 19 to deploy these patches on machines running on these operation systems.