Informe de análisis de riesgo en servidores

Julio 2017

Realizado por:
Trend Micro

Contenido

Resumen Ejecutivo

Tras realizar un análisis de riesgo en los servidores seleccionados, identificamos más de **2,959 vulnerabilidades** en **X servidores** de distintos grados de criticidad de acuerdo a los estándares de seguridad.

Algunas de estas vulnerabilidades pueden ser explotadas para permitir el **Secuestro de Información, Exposición ante ransomware "Wannacry" e incluso pueden comprometer el acceso y operación de las aplicaciones** alojadas en dichos servidores.

2,745 de estas vulnerabilidades comprometen directamente la operación de estos servidores, permitiendo el control total de ellos por parte de un tercero, o bien provocando el bloqueo total de la operación de las aplicaciones y servicios asociados a ellos.

El principal riesgo se ubica en el servidor que aloja la aplicación XXX que es crítica para la operación de la empresa, ya que forma parte fundamental del proceso de manejo de clientes.

La siguiente matriz de riesgo tabula el nivel de criticidad de las vulnerabilidades encontradas VS. el número de vulnerabilidades de cada uno de los sistemas.

	Nombre de Servidor					
Riesgo de impacto en la operación	WEB SERVER LINUX	WEB SERVER WIN2K8	INTERFAZ LINUX-WIN	EXTRANET	DNS Externo	XXX
Secuestro de información confirmada						
Riesgo inminente ante Ransomware WannaCry	1	1	1		1	1
Operación en riesgo critico ante compromiso del servidor	690	762	195	124	650	182
Operación en riesgo alto ante denegación de servicio	19	23	29	3	22	23
Información en riesgo de ser suplantada/eliminada	35	57	34	15	56	32
Posibilidad de modificación de parametros de operación	1	1	2		2	2

Realizar una remediación manual de estas vulnerabilidades, requeriría de la implementación de **2,959 parches de seguridad de distintos fabricantes**[1] que, tomando como base que la implementación de cada uno de ellos requiere de una ventana de mantenimiento de entre 30 minutos y 2 horas, se estima un mínimo de **1,500 horas de no disponibilidad y no operación.**

[1] Gran parte de estos parches de seguridad, no podrán ser implementados debido a que pertenece a sistemas no soportados por sus fabricantes (ej. Microsoft Windows Server 2003).

La Solución propuesta por Trend Micro ante esta problemática se basa en la implementación del control compensatorio de **"Parcheo Virtual" (Trend Micro Deep Security),** que evita que las vulnerabilidades de seguridad descubiertos sean explotadas y/o utilizados por cibercriminales.

El esfuerzo invertido para implementar este control **no excederá de las 2 horas hombre y la no disponibilidad de las aplicaciones** (ventana de mantenimiento de instalación).

Análisis Técnico

A continuación, se muestran los resultados obtenidos durante la ejecución del análisis de riesgos en los servidores realizada el (FECHA).

RESULTADOS DEL ANÁLISIS DE VULNERABILIDADES
Después de realizar el análisis de vulnerabilidades en el servidor encontramos un total de **2,959 maneras de afectar, parcial o totalmente la operación**, de las cuales 2603 son críticas.

A continuación, se muestra un resumen de éstas vulnerabilidades por servidor y la criticidad de las mismas:

		Riesgo de la Vulnerabilidad				
Servidor	**Rol del Servidor**	**Bajo**	**Medio**	**Alto**	**Critico**	**Total**
A	DNS EXT	2	56	22	650	**730**
B	APLICACIÓN XXX	2	32	23	182	**239**
C	INTERFACES LINUX-WINDOWS	2	34	29	195	**260**
D	WEB SERVER	1	35	19	690	**745**
E	WEB SERVER	1	57	23	762	**843**
F	EXTRANET	0	15	3	124	**142**

Ejemplo vulnerabilidades críticas encontradas:

En días pasados ocurrió un ataque de **Ransomware** de alcance masivo con **mecanismos de auto-propagación** que afecto potencialmente a los **sistemas operativos Windows,** cifrando archivos y pidiendo rescate para recuperar la información encriptada. Este ataque ha afectado a muchas empresas alrededor del mundo y hemos recibido varios reportes de empresas en Latinoamérica.

El ataque utiliza una **variante de Ransomware** denominada"**WannaCry**" y sabemos que esta amenaza explota una vulnerabilidad de varios sistemas operativos Microsoft Windows para propagarse.

Esta vulnerabilidad fue descubierta el pasado 14 de Marzo de 2017 y se detalla en el siguiente boletín de Microsoft: https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

MS17-010	
Resumen ejecutivo	Esta actualización resuelve vulnerabilidades en Microsoft Windows. La más grave de estas vulnerabilidades podría permitir la ejecución remota de código si un atacante envía mensajes especialmente diseñados a un servidor de Microsoft Server Message Block 1.0 (SMBv1).
Fecha de Liberación	14 de Marzo
¿Requiere Reinicio?	Si
Vector de Acceso	A través de red, puerto 445
Vectores de ataque	Un atacante no autenticado podría enviar una solicitud de autenticación especialmente diseñada.
Factores mitigadores	Actualización de seguridad MS17-010
Tipo de impacto	• Compromiso total de la integridad del sistema • Compromiso total de la confidencialidad del sistema • Compromiso total de la disponibilidad del sistema
Software afectado	• Windows Vista • Windows Server 2008 • Windows 7 • Windows Server 2008 R2

	• Windows 8.1 • Windows Server 2012 and Windows Server 2012 R2 • Windows RT 8.1 • Windows 10 • Windows Server 2016

Esta vulnerabilidad fue descubierta en los siguientes servidores:

Hostname/IP	Rol del Servidor	vulnerable a MS17-010 (Wanna cry)
Alfa	DNS EXT	**Si**
Beta	APLICACIÓN XXX	**Si**
Gama	INTERFACES LINUX-WINDOWS	**Si**
Omega	WEB SERVER	**Si**
Kappa	WEB SERVER	**Si**
Epsilon	EXTRANET	No

Conclusiones

Al finalizar el análisis de riesgo en los servidores, podemos extraer varias conclusiones de importancia:

- El riesgo de detener la operación es sumamente alto debido a la cantidad y criticidad de las vulnerabilidades encontradas.
- Gran parte de estas vulnerabilidades pertenecen a sistemas no soportados por el fabricante o en servidores con operación 7/24, imposibilitando la implementación del parche correspondiente.

Contactos Trend Micro

Nombre	Rol	Correo
Name	Regional Account Manager	name_lastname@trendmicro.com
Name	Regional Account Manager	name_lastname@trendmicro.com
Name	Sales Engineer	name_lastname@trendmicro.com

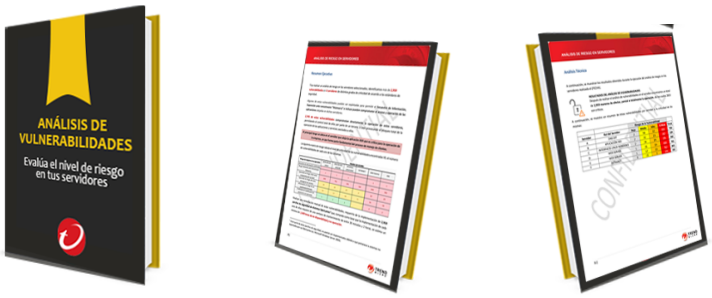
El primer paso para defenderte es conocer el riesgo de tus sistemas.

UN NUEVO ENFOQUE DE PROTECCIÓN DE LA INFORMACIÓN

En la era de la movilidad, la consumerización, la computación basada en la nube y los ataques dirigidos, nos sobran los motivos para estar preocupados por la seguridad y la protección de nuestros datos. Por lo tanto, las soluciones de seguridad deben modificar su modelo de defensa hacia un enfoque de protección dinámico y flexible mientras la información se desplaza entre entornos físicos, virtuales y basados en la nube.

En Grupo Smartekh estamos conscientes de esta evolución y en conjunto con Trend Micro queremos ayudarte a reducir la superficie de ataque en cualquiera de estos entornos a través de la identificación de vulnerabilidades críticas en tus servidores.

Reservar mi Análisis Gratuito de Vulnerabilidades



TREND MICRO | Grupo Smartekh

PARTNER PLATINUM

WWW.SMARTEKH.COM

http://info.smartekh.com/analisis-de-vulnerabilidades-en-servidores