proactive
Information security.

Ayudamos a Proteger sus Activos de Información

ProActive News Vol.3

Agosto 2017

¿Podría haber un ciber ataque del tipo Wannacry nuevamente?

La respuesta, lastimosamente, es **SI**. La semana pasada Microsoft hacia públicos sus parches de seguridad, como todos los segundos martes de cada mes, los cuales solucionan un total de 48 vulnerabilidades en los sistemas Windows, 25 de las cuales están consideradas como criticas.

Rememorando el caso ***Wannacry***, para no caer en el mismo error o aprender de la experiencia anterior, el parche liberado por Microsoft que solucionaba este problema se seguridad fue publicado en el mes de Marzo de 2017. Dos meses después salía a la luz ***Wannacry***, y tuvo tal nivel de propagación debido a que los usuarios y las empresas no tenían sus sistemas actualizados.

La vulnerabilidad actual, calificada como critica, afecta a todas las versiones de **Windows Search**, el buscador de Windows, la cual hace que todas las versiones del sistema operativo, desde Windows 7 a Windows 10 sean vulnerables.

La misma ha sido registrada como **CVE-2017-8620 "Windows Search Remote Code Execution Vulnerability".** Este fallo de seguridad puede permitir a un atacante realizar búsquedas a través del buscador de Windows, y, en vez de archivos y contenidos del disco duro, puede acceder a entradas directamente en la memoria RAM, lo que puede permitir tomar el control completo de cualquier sistema vulnerable y utilizarlo, por ejemplo, para ejecutar código arbitrario o instalar malware, entre otros fines.

¿Qué sistemas se ven afectados?

- Windows Server 2008 SP2 y R2 SP1
- Windows 7 SP1
- Windows 8.1
- Windows Server 2012 Gold y R2
- Windows RT 8.1
- Windows 10 Gold, 1511, 1607 y 1703
- Windows Server 2016

Referencia:

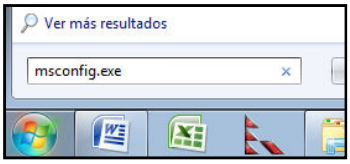
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8620

¿Cómo evito este problema de seguridad?

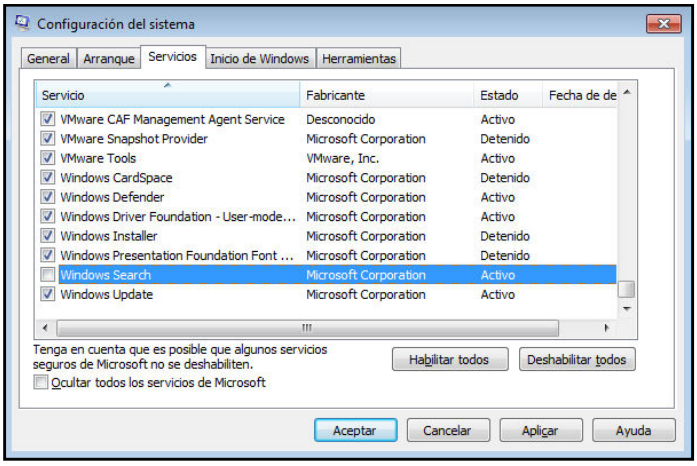
En lo particular se puede mitigar esta vulnerabilidad desactivando `Windows Search` en los equipos afectados:

Método 1

1. Ejecutar el comando `msconfig.exe`

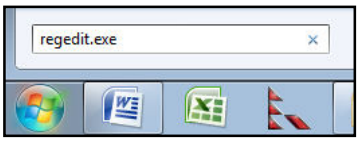


2. Deshabilitar `Windows Search`

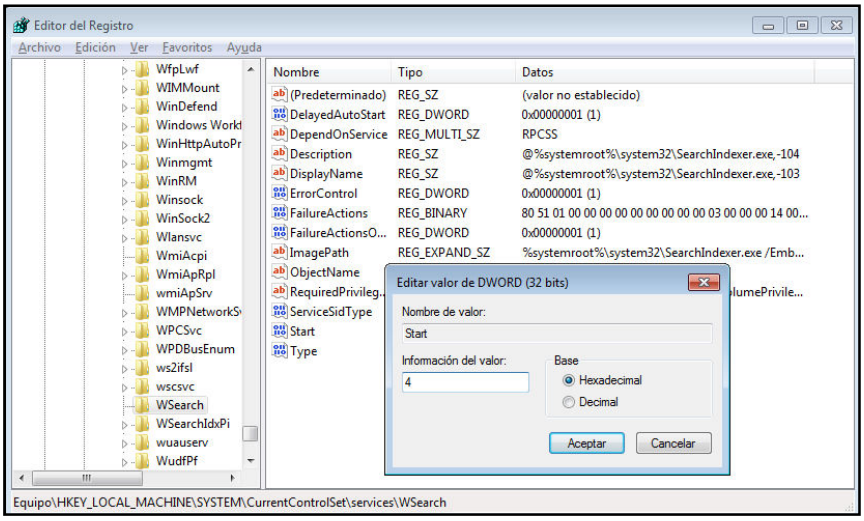


Método 2

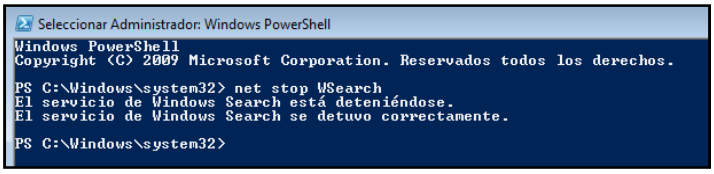
1. Ejecutar el comando `regedit.exe`



2. Buscaremos la entrada "`Start`" en la ruta "`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WSearch`" del Registro de Windows y la asignaremos el valor 4.



3. Una vez hecho esto, abriremos una ventana de `PowerShell` como Administrador y ejecutaremos el comando "`net stop WSearch`" para detener el servicio.



En lo general las recomendaciones son:

1. Estar al día con todas las actualizaciones (parches) de seguridad publicados por el proveedor del software, en este caso Microsoft.
2. La copia de respaldo frecuente (*backup*) de la información es fundamental.
3. La concientización de usuarios en el ámbito de Seguridad de la Información ayuda bastante a mitigar los riesgos asociados a las amenazas y vulnerabilidades existentes.

Con objeto de mantenerlo actualizado y protegido, quedamos a vuestra disposición para asesorarlo en cuanto a la detección de vulnerabilidades en su plataforma que puedan ser explotadas.

Obtenga mayor información sobre nuestros servicios y productos, póngase en contacto con nosotros:

Web: www.proactive.consulting

Mail: contacto@proactive.consulting

Tel: +595 (981) 478-921

Twitter: @ProActive_py