Investigadores de seguridad cibernética publicaron hoy el código de prueba de concepto (PoC) para explotar una vulnerabilidad recientemente parcheada en el sistema operativo Windows, misma que fue informada a Microsoft por la Agencia de Seguridad Nacional de Estados Unidos (NSA).

La vulnerabilidad, denominada como CurveBall, afecta a CryptoAPI (Crypt32.dll), el componente que maneja las operaciones criptográficas en el sistema operativo Windows.

Según un análisis técnico de alto nivel del error, por parte del investigador Tal Be'ery, *«la causa raíz de esta vulnerabilidad es una implementación defectuosa de la criptografía de curva elíptica (ECC) dentro del código de Microsoft».*

Según la NSA, el DHS y Microsoft, cuando se explota la vulnerabilidad, puede permitir que un atacante realice las siguientes acciones:

- Lanzar ataques MitM (man-in-the-middle) e interceptar y falsificar conexiones HTTPS
- Firmas falsas para archivos y correos electrónicos
- Código falso ejecutable firmado ejecutado dentro de Windows

Mientra tanto, el asesor interino de Seguridad Nacional, Rob Joyce, dijo en Twitter que se trata de un error *«muy mal»*.

Las autoridades estadounidenses reaccionaron a la vulnerabilidad de forma muy abierta y proactiva. La NSA lanzó una rara alerta de seguridad sobre el error, y el departamento CISA del DHS emitió una directiva de emergencia, dando a las agencias gubernamentales diez días para parchear los sistemas mediante la aplicación de las actualizaciones del martes de parches de Microsoft 2020 de enero del mismo año.

Esta es la primera vez que la NSA informa un error a Microsoft. Se podría decir que la agencia está en una gira de prensa para mejorar su imagen en la comunidad de seguridad cibernética luego de los desastres de EternalBlue y Shadow Brokers, cuando las herramientas de piratería desarrolladas por la NSA se filtraron en línea y se usaron para algunas de las

mayores infecciones de malware y ataques cibernéticos conocidos hasta ahora.

Expertos en seguridad y criptográficos experimentados como Thomas Ptacek y Kenneth White, confirmaron la gravedad y el amplio impacto de la vulnerabilidad, aunque no afecta el mecanismo de actualización de Windows, lo que habría permitido que un actor de amenazas falsifique las actualizaciones de Windows.

## Prueba de Concepto

En una publicación de blog del martes pasado, White dijo que estaba al tanto de que algunas personas estaría cerca de encontrar un exploit para la vulnerabilidad CurveBall.

El primero en llegar fue Saleem Rashid, quien creó un código de prueba de concepto para falsificar certificados TLS y permitir que los sitios se hagan pasar por legítimos.

Rashid no publicó su código, pero otras personas sí algunas horas después. El primer exploit CurveBall público provino de Kudelski Security, seguido por un segundo de un investigador de seguridad danés que se llamaba Ollypwn.

En el aviso de seguridad oficial para CVE-2020-0601, Microsoft describió la posibilidad de que los actores de amenazas exploten el error como *«más probable».* Con el código de demostración público disponible, las posibilidades de explotación ahora también están aseguradas.

La buena noticia en todo esto es que aún si los usuarios no han tenido tiempo de programar el tiempo para instalar los parches, Windows Defender recibió actualizaciones para al menos detectar intentos de explotación activa y advertir a los usuarios. Según Microsoft, esta vulnerabilidad afecta a las versiones del sistema operativo Windows 10, Windows Server 2019 y Windows Server 2016.