Microsoft publicó sus parches de seguridad de enero ayer, advirtiendo a millones de usuarios sobre 49 nuevas vulnerabilidades en su familia de productos.

Uno de los aspectos más importantes de este Patch Tuesday, es una actualización que corrige una vulnerabilidad grave en el componente criptográfico central de las ediciones ampliamente utilizadas de Windows 10, Windows Server 2016 y 2019, que fue descubierta e informada a la compañía por la Agencia de Seguridad Nacional de Estados Unidos (NSA).

Esta sería la primera falla de seguridad en el sistema operativo Windows que la NSA informa de forma responsable a Microsoft, a diferencia de la vulnerabilidad EternalBlue SMB, que la agencia mantuvo en secreto por al menos cinco años y luego fue filtrada al público por un grupo misterioso, lo que causó la amenaza global de WannaCry en 2017.

Vulnerabilidad de suplantación de identidad de Windows CryptoAPI

Según un aviso publicado por Microsoft, la falla, denominada como NSACrypt y rastreada como CVE-2020-0601, reside en el módulo Crypt32.dll, que contiene diversas *«funciones de certificado y mensajería criptográfica»* utilizadas por la API Crypto de Windows para manejar el cifrado de datos.

El problema reside en la forma en que el módulo Crypt32.dll valida los certificados de criptografía de curva elíptica (ECC), que actualmente es el estándar de la industria para la criptografía de clave pública y se utiliza en la mayoría de los certificados SSL/TLS.

En un comunicado de prensa publicado por la NSA, la agencia explica que *«la vulnerabilidad de validación de certificados permite a un atacante socavar cómo Windows verifica la confianza criptográfica y puede permitir la ejecución remota de código».*

Los hackers que logren explotar la vulnerabilidad, podrán abusar de la validación de confianza entre:

- Conexiones HTTPS
- Archivos firmados y correos electrónicos
- Código ejecutable firmado lanzado como procesos en modo de usuario

Aunque los detalles técnicos de la falla aún no están disponibles al público, Microsoft confirmó que la falla, de ser explotada con éxito, podría permitir a los hackers falsificar firmas digitales en el software, engañando al sistema operativo para que instale software malicioso mientras se hace pasar por la identidad de cualquier software legítimo.

> *«Existe una vulnerabilidad de suplantación de identidad en la forma en que Windows CryptoAPI (Crypt32.dll) valida los certificados de criptografía de curva elíptica (ECC)»,* dice Microsoft.
>
> *«Un atacante podría explotar la vulnerabilidad mediante el uso de un certificado de firma de código falsificado para firmar un ejecutable malicioso, haciendo que parezca que el archivo proviene de una fuente confiable y legítima. El usuario no tendría forma de saber que el archivo es malicioso porque la firma digital parecería ser de un proveedor de confianza».*

Además, la falla en CryptoAPI también podría hacer que los atacantes remotos intermedios, se hagan pasar por sitios web o descifrar información confidencial sobre las conexiones de los usuarios con el software afectado.

> *«Esta vulnerabilidad está clasificada como importante y no la hemos visto utilizada en ataques activos»,* dice Microsoft en una publicación separada.
>
> *«Esta vulnerabilidad es un ejemplo de nuestra asociación con la comunidad de investigación de seguridad en la que se divulgó una vulnerabilidad de forma privada*

> *y se lanzó una actualización para garantizar que los clientes no estuvieran en riesgo»,* agregó.
>
> *«Las consecuencias de no reparar la vulnerabilidad son graves y generalizadas. Las herramientas de explotación remota probablemente estarán disponibles de forma rápida y generalizada»,* dijo la NSA.

Aparte de la vulnerabilidad de suplantación de identidad de Windows, CryptoAPI, Microsoft también parcheó otras 48 vulnerabilidades, de las cuales, ocho son críticas y el resto son importantes.

No existe mitigación o solución disponible para esta vulnerabilidad, por lo que se recomienda instalar las últimas actualizaciones de software para Windows.

Por otro lados, de las fallas críticas descubiertas, dos afectan a Windows Remote Desktop Gateway (RD Gateway), rastreado como CVE-2020-0609 y CVE-2020-0610, que pueden ser explotados por atacantes no autenticados para ejecutar código malicioso en sistemas específicos simplemente enviando una solicitud especialmente diseñada por medio de RDP.

> *«Esta vulnerabilidad es una autenticación previa y no requiere la interacción del usuario. Un atacante que aproveche esta vulnerabilidad podría ejecutar código arbitrario en el sistema de destino»*, dice el aviso.

Otro problema crítico en Remote Desktop Cliente, rastreado como CVE-2020-0611, podría conducir a un ataque RDP inverso donde un servidor malicioso puede ejecutar código arbitrario en la computadora del cliente que se conecta.

> *«Para explotar esta vulnerabilidad, un atacante necesitaría tener el control de un*

> *servidor y luego convencer a un usuario para que se conecte a él. Un atacante también podría comprometer un servidor legítimo, alojar código malicioso en él y esperar a que el usuario se conecte»,* dice el aviso.

Por fortuna, ninguna de las vulnerabilidades abordadas este mes fueron reveladas públicamente ni se descubrieron explotaciones en la naturaleza.