UNIVERSIDAD CATÓLICA DE CÓRDOBA
JESUITAS

SISTEMAS OPERATIVOS
TRABAJO PRÁCTICO N°1

Profesor: Lic. Gustavo A. Funes.

Alumnos: Cerrutti Angie Lucia (1901510), Folco Juan Ignacio (1912673), Menel Angelo (1804789), Vietto Santiago (1802890)

Fecha: 16/08/2022

Desarrollo

Descripción del problema

En 2020, la Agencia de Seguridad Nacional de Estados Unidos (NSA) descubrió una falla dentro de las funcionalidades de Windows 10, la cual puede ser aprovechada por ciberdelincuentes para crear software malicioso que simule o parezca ser legítimo. Dicha falla se explota a través de un componente central de Windows conocido como **crypt32.dll**, el cual es un programa que permite a los desarrolladores de software acceder a varias funciones, como por ejemplo, los certificados digitales que se usan para firmar software.

Existe una vulnerabilidad de suplantación de identidad (spoofing) en la forma en que Windows CryptoAPI (Crypt32.dll) valida los certificados de criptografía de curva elíptica (Elliptic Curve Cryptography - ECC). Un atacante podría aprovechar 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 legítima y confiable. El usuario no tendría forma de saber que el archivo es malicioso, porque la firma digital parecería ser de un proveedor confiable. Una explotación exitosa también podría permitir al atacante realizar ataques de tipo man-in-the-middle y descifrar información confidencial sobre las conexiones de los usuarios al software afectado. Solo se ven afectadas las versiones de Windows 10 del sistema operativo, ya que en la versión inicial de Windows 10, Microsoft agregó compatibilidad con los parámetros ECC que configuran las curvas ECC. Antes de esto, Windows solo admitía curvas ECC con nombre. El código que agregó soporte para parámetros ECC también resultó en la vulnerabilidad de validación de certificados. No fue una regresión, y las versiones de Windows que no son compatibles con los parámetros ECC que configuran las curvas ECC, como Servers, 2008, Windows 7, Windows 8.1 y servers, no se vieron afectadas. A continuación vemos algunas métricas del ataque:

Contexto en el que es posible la explotación:	El componente vulnerable está vinculado a la network slack y el conjunto de posibles atacantes se extiende más allá de las otras opciones enumeradas, hasta incluir todo Internet. Dicha vulnerabilidad a menudo se denomina “remotely exploitable” (explotable de forma remota) y puede considerarse como un ataque explotable a nivel de protocolo uno o más saltos de red.
Complejidad del ataque:	Bajo, ya que no existen condiciones especiales de acceso ni circunstancias atenuantes. Un atacante puede esperar

	un éxito repetible contra el componente vulnerable.
Requerimientos de privilegios:	El atacante no está autorizado antes del ataque y, por lo tanto, no requiere ningún acceso a la configuración o los archivos para llevar a cabo un ataque.
Interacción del usuario (no atacante):	La explotación exitosa de esta vulnerabilidad requiere que el usuario realice alguna acción antes de que se pueda explotar la vulnerabilidad.
Alcance:	El componente vulnerable y el componente afectado son el mismo o ambos están administrados por la misma autoridad de seguridad.
Confidencialidad:	Hay pérdida total de confidencialidad, lo que da como resultado que todos los recursos dentro del componente afectado se divulguen al atacante.
Integridad:	Hay una pérdida total de integridad, o una pérdida completa de protección. Por ejemplo, el atacante puede modificar cualquiera o todos los archivos protegidos por el componente afectado.
Disponibilidad:	No hay impacto en la disponibilidad dentro del componente afectado.

Otras métricas:

Exploit Code Maturity	El código o la técnica no es funcional en todas las situaciones y puede requerir una modificación sustancial por parte de un atacante experto.
Remediation Level:	Se encuentra disponible una solución de proveedor completa. Microsoft ha emitido un parche oficial, o hay una actualización disponible.
Report Confidence:	El código fuente está disponible para verificar de forma independiente las afirmaciones de la investigación, o el autor o proveedor del código afectado

	ha confirmado la presencia de la vulnerabilidad.

Las autoridades solicitaron de forma inmediata la aplicación de un parche para la solución del mismo, en donde aclararon que aquellos dispositivos que no realicen la actualización correspondiente serán los principales objetivos de ataques. La actualización de seguridad corrige la vulnerabilidad al garantizar que Windows CryptoAPI valide completamente los certificados ECC.

Especificaciones Técnicas

• Sistema operativo, plataforma y requerimientos (hard):

Windows 10; **Universal Windows Platform/UWP;** requerimientos mínimos:

- **Procesador:** de 1 gigahercio (GHz), o procesador o SoC más rápido
- **RAM:** 1 gigabyte (GB) para 32 bits o 2 GB para 64 bits
- **Espacio en disco duro:**16 GB para el sistema operativo de 32 bits o 20 GB para el sistema operativo de 64 bits
- **Tarjeta gráfica:** DirectX 9 o posterior con controlador WDDM 1.0
- **Pantalla:** 800 x 600

• Objetivo del tipo de Sistema Operativo:

El sistema operativo está diseñado para ser una nueva dirección para Microsoft. Uno de los principales objetivos de Windows 10 es unificar la experiencia de Windows en múltiples dispositivos, como ordenadores de sobremesa, tabletas y smartphones.

Las metas de este modelo fue reducir la fragmentación en toda la plataforma de Windows.

• Aplicaciones que pueden soportar y dónde se usa:

Windows 10 es un sistema operativo que se utiliza para juegos, herramientas de oficina (paquete de Office), edición de multimedia, y uso de demás aplicaciones diseñadas para el mismo.

Windows 10 favorece la simplicidad al usuario final, permitiendo una personalización más amplia de su experiencia.

• Costos:

Los costos que una implementación exitosa de esta vulnerabilidad habría causado podrían haber sido graves, a nivel de millones, dado que afecta al sistema de confianza de las aplicaciones instaladas.

En la práctica, no han habido pérdidas dado que la vulnerabilidad fue solucionada con un parche antes de dar a luz.

Fuentes de información

https://www.prensalibre.com/vida/tecnologia/la-falla-de-seguridad-de-windows-10-detectada-por-el-gobierno-de-ee-uu-que-pone-en-riesgo-a-millones-de-computadoras-2/

https://support.microsoft.com/es-es/windows/requisitos-del-sistema-de-windows-10-6d4e9a79-66bf-7950-467c-795cf0386715

https://techterms.com/definition/windows_10

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-0601

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0601

https://techmonitor.ai/technology/cybersecurity/crypt32-dll-vulnerability-nsa