Mozilla ha implementado soluciones para abordar una vulnerabilidad de seguridad crítica en su biblioteca criptográfica de servicios de seguridad de red (NSS) multiplataforma, que podría ser explotada por un hacker para bloquear una aplicación vulnerable e incluso ejecutar código arbitrario.

Rastreada como CVE-2021-43527, la vulnerabilidad afecta a las versiones NSS anteriores a 3.73 o 3.68.1 ESR y se refiere a una vulnerabilidad de desbordamiento de pila al verificar firmas digitales como los algoritmos DSA y RSA-PSS que están codificados usando el formato binario DER.

Tavis Ormandy de Google Project Zero, quien lo nombró BigSig, fue quien informó sobre el problema.

> *«Las versiones de NSS (Network Security Services) anteriores a 3.73 o 3.68.1 ESR son vulnerables a un desbordamiento de pila cuando se manejan firmas DSA o RSA-PSS codificadas en DER. Las aplicaciones que usan un NSS para manejar firmas codificadas dentro de CMS, S/MIME, PKCS #7 o PKCS #12 probablemente se vean afectadas»,* dijo Mozilla.

NSS es una colección de bibliotecas informáticas criptográficas de código abierto diseñadas para permitir el desarrollo multiplataforma de aplicaciones cliente-servidor, con soporte para SSL v3, TLS, PKCS #5, PKCS #7, PKCS #11, PKCS #12, S/Certificados MIME, X.509 v3 y otros estándares de seguridad.

Se cree que el error, consecuencia de una verificación de límites faltantes que podría permitir la ejecución de código arbitrario controlado por el atacante, se puede explotar desde junio de 2012.

> *«Lo sorprendente de esta vulnerabilidad es lo simple que es. Este problema demuestra que incluso C/C++ extremadamente bien mantenido puede tener*

> *errores fatales y triviales»*, dijo Ormandy.

Aunque la deficiencia de BigSig no afecta al navegador web Firefox de Mozilla, se cree que los clientes de correo electrónico, los visores PDF y otras aplicaciones que dependen de NSS para verificación de firmas, como RedHat, Thunderbird, LibreOffice, Evolution y Evince, son vulnerables.

> *«Esta es una falla importante de corrupción de memoria en NSS, casi cualquier uso de NSS se ve afectado. Si usted es un proveedor que distribuye NSS en sus productos, lo más probable es que necesite actualizar el parche»*, dijo Ormandy.