BOLETÍN DE ALERTA

Boletín Nro.: 2022-18

Fecha de publicación: 17/03/2022

Tema: Vulnerabilidad de denegación de servicio (DoS) en OpenSSL.

Versiones afectadas de OpenSSL:

- OpenSSL, versión 1.0.2.
- OpenSSL, versión 1.1.1.
- OpenSSL, versión 3.0.

Descripción:

Se han publicado actualizaciones de seguridad que subsanan una vulnerabilidad de severidad alta en OpenSSL, por la que un error podría provocar un bucle infinito, permitiendo así a un atacante realizar denegación de servicio (DoS).

La vulnerabilidad CVE-2022-0778 de severidad alta, sin una puntuación asignada aún. Esta se debe a que la función *BN_mod_sqrt()*, que calcula una raíz cuadrada modular, contiene un error que podría provocar un bucle infinito para módulos no primos. Sería posible desencadenar el bucle infinito si se crea un certificado que tiene parámetros de curva explícitos no válidos.

Adicionalmente, cualquier otra aplicación que utilice la función *BN_mod_sqrt()*, donde el atacante pudiera controlar los valores de los parámetros, serían vulnerables a esta condición de denegación de servicio (DoS). En particular, el atacante puede usar un certificado autofirmado para activar el bucle durante la verificación de la firma del certificado.

Impacto:

La explotación de esta vulnerabilidad permitiría a un atacante realizar un ataque de denegación de servicio (DoS).

Detección:

Verificar si se posee instalado la versión afectada en el equipo.

- OpenSSL, versión 1.0.2.
- OpenSSL, versión 1.1.1.
- OpenSSL, versión 3.0.

También verificar si se encuentran en las siguientes situaciones vulnerables:

- Clientes TLS que consumen certificados de servidor.
- Servidores TLS que consumen certificados de clientes.
- Proveedores de alojamiento que recogen certificados o claves privadas de los clientes.
- Autoridades de certificación que analizan las solicitudes de certificación de los suscriptores.
- Cualquier otro componente que analice parámetros de curva elíptica ASN.1.

Solución:

Recomendamos instalar las actualizaciones correspondientes provistas por OpenSSL, mediante los siguientes enlaces, según su distribución:

Open 1.0.2zd, está disponible para clientes de soporte premium:

- https://www.openssl.org/support/contracts.html

OpenSSL, versión 1.1.1n:

- https://www.openssl.org/source/openssl-1.1.1n.tar.gz

OpenSSL, versión 3.0.2:

- https://www.openssl.org/source/openssl-3.0.2.tar.gz

Información adicional:

- https://www.openssl.org/news/secadv/20220315.txt
- https://nvd.nist.gov/vuln/detail/CVE-2022-0778
- https://www.incibe-cert.es/alerta-temprana/avisos-seguridad/bucle-infinito-openssl
- https://www.openssl.org/source/