El Proyecto OpenSSL publicó correcciones para abordar varias vulnerabilidades de seguridad, incluyendo un error de alta gravedad en el conjunto de herramientas de cifrado de código abierto que podrían exponer a los usuarios a ataques maliciosos.

Rastreada como CVE-2023-0286, la vulnerabilidad se relaciona con un caso de confusión de tipos que puede permitir que un atacante *«lea el contenido de la memoria o promulgue una denegación de servicio»*, dijeron los mantenedores en un aviso.

La vulnerabilidad tiene sus raíces en la forma en que la popular biblioteca criptográfica maneja los certificados X.509 y es probable que afecte solo a aquellas aplicaciones que tienen una implementación personalizada para recuperar una lista de revocación de certificados (CRL) por medio de una red.

> *«En la mayoría de los casos, el ataque requiere que el atacante proporcione tanto la cadena de certificados como la CRL, ninguno de los cuales necesita tener una firma válida. Si el atacante solo controla una de estas entradas, la otra entrada ya debe contener una dirección X.400 como punto de distribución de CRL, lo cual es poco común»*, dijo OpenSSL.

Las vulnerabilidades de confusión de tipos podrían tener consecuencias graves, ya que podrían convertirse en armas para obligar deliberadamente al programa a comportarse de forma no deseada, lo que posiblemente provoque un bloqueo o la ejecución del código.

El problema se solucionó en las versiones 3.0.8, 1.1.1t y 1.0.2zg de OpenSSL. Otras fallas de seguridad abordadas como parte de las últimas actualizaciones incluyen:

- CVE-2022-4203: Restricciones de nombre X.509, desbordamiento del búfer de lectura
- CVE-2022-4304: Sincronización de Oracle en el descifrado RSA
- CVE-2022-4450: Doble after-free al llamar a PEM_read_bio_ex
- CVE-2023-0215: Use-after-free siguiendo BIO_new_NDEF
- CVE-2023-0216: Eliminación de referencia de puntero no válida en funciones

d2i_PKCS7
- CVE-2023-0217: Desreferencia NULL que valida la clave pública de DSA
- CVE-2023-0401: Desreferencia NULL durante la verificación de datos PKCS7

La explotación exitosa de las deficiencias anteriores podría provocar un bloqueo de la aplicación, revelar el contenido de la memoria e incluso recuperar mensajes de texto sin formato enviados a través de una red aprovechando un canal lateral basado en el tiempo en lo que es un ataque de estilo Bleichenbacher.

Las correcciones llegan casi dos meses después de que OpenSSL corrigió una vulnerabilidad de baja gravedad (CVE-2022-3996) que surge al procesar un certificado X.509, lo que genera una condición de denegación de servicio.