BOLETÍN DE ALERTA

Boletín Nro.: 2020-11
Fecha de publicación: 23/04/2020
Tema: Actualización de seguridad para OpenSSL aborda vulnerabilidad de riesgo alto.

- CVE-2020-1967.

Sistemas afectados:

- OpenSSL en sus versiones **1.1.1d**, **1.1.1e** y **1.1.1f**

Descripción:

Recientemente **OpenSSL** ha lanzado un aviso de seguridad donde informa la corrección de una vulnerabilidad de **alto riesgo**. Este fallo se encuentra en la función **SSL_check_chain()**, y es debido a un **error de segmentación** en las aplicaciones de servidor o de cliente que invocan a esta **función**, durante o después del proceso de **Handshake TLS 1.3 (proceso de comunicación)**, un atacante podría aprovechar esto para enviar una solicitud con un algoritmo no **válido** o no **reconocido** por el par, causando una desreferencia de puntero **null** en la extensión **TLS signature_algorithms_cert** y seguidamente un bloqueo de la comunicación.

La vulnerabilidad en cuestión no afecta a versiones anteriores de **OpenSSL (1.0.2 y 1.1.0)**. Sin embargo, dichas versiones ya no cuentan con actualizaciones de seguridad.

Impacto:

Esta vulnerabilidad podría permitir a un atacante remoto realizar un ataque de **denegación de servicios (DoS).**

Solución y prevención:

- Actualizar OpenSSL a la versión 1.1.1g**.**
- En caso de contar con versiones anteriores a 1.0.2 o 1.1.0, se recomienda actualizar a la última versión disponible. Esto debido a que dichas versiones ya **no cuentan** con actualizaciones de seguridad.

Información adicional:

- https://www.openssl.org/news/secadv/20200421.txt
- https://www.incibe-cert.es/alerta-temprana/avisos-seguridad/vulnerabilidad-fallo-segmentacion-sslcheckchain-openssl
- https://securityaffairs.co/wordpress/101997/security/openssl-cve-2020-1967-dos-issue.html
- https://www.securitynewspaper.com/2020/04/22/how-to-exploit-openssl-to-do-dos-attack-cve-2020-1967/