USTIC-AV 18/22. Vulnerabilidades de severidad alta en OpenSSL (07/11/2022)

La **Unidad de Seguridad TIC** de la Subdirección de Tecnologías de la Información y Comunicaciones **avisa** de la **publicación** de **dos vulnerabilidades de severidad alta en OpenSSL** que **podrían permitir** a un atacante causar una condición de **denegación de servicio o** realizar una **ejecución remota de código**.

Detalle

OpenSSL es una biblioteca de criptografía de código abierto ampliamente utilizada por aplicaciones, sistemas operativos y sitios web para asegurar las comunicaciones a través de Internet utilizando SSL (*Secure Sockets Layer*) y TLS (*Transport Layer Security*).

Los investigadores, Polar Bear y Viktor Dukhovni, han reportado 2 vulnerabilidades de severidad alta que afectan a esta biblioteca que podrían permitir a un atacante causar una condición de denegación de servicio o realizar una ejecución remota de código.

Los dos fallos de seguridad publicados se producen al realizar la comprobación de restricciones de nombres durante la verificación de certificados X.509, ya que se podría producir un desbordamiento de búfer. Un atacante podría crear una dirección de correo electrónico maliciosa para desbordar 4 bytes controlados en la pila (CVE-2022-3602) o para desbordar un número arbitrario de bytes que contengan el carácter '.' correspondiente al valor 46 en decimal (CVE-2022-3786).

Ambas vulnerabilidades podrían producirse en un cliente TLS al conectarse a un servidor malicioso. En un servidor TLS, podrían desencadenarse si el servidor solicita la autenticación del cliente, y se conecta un cliente malicioso.

Recursos Afectados

Las versiones 3.0.0 y superiores de OpenSSL son vulnerables. La mayoría de las implementaciones de OpenSSL que se utilizan hoy en día emplean la versión 1.1.1 o 1.0.2; sin embargo, OpenSSL 3 se incluye en muchas versiones de Linux, como RedHat, Fedora, CentOS, Linux Mint y otras.

Los contenedores Docker suelen incluir alguna versión de OpenSSL, pero qué versión y si es vulnerable dependerá de la configuración original. La biblioteca también puede instalarse opcionalmente en dispositivos macOS y Windows, aunque por defecto los Macs ejecutan la biblioteca LibreSSL, que no está afectada. Las versiones vulnerables de OpenSSL también se utilizan en software de desarrollo popular como Gradle, herramientas de privacidad como TOR y plataformas de seguridad como Kali Linux.

El NCSC-NL (Centro Nacional de Ciberseguirdad holandés) ha publicado un listado con información sobre las versiones incluidas por varios fabricantes.

Vulnerable

- **OpenSSL 3.0.0 hasta 3.0.6**

No vulnerable

- OpenSSL 1.1.1
- OpenSSL 1.1.0
- OpenSSL 1.0.2
- OpenSSL 1.0.1
- LibreSSL

Recomendaciones Actualizadas (07/11/2022)

La Unidad de Seguridad TIC de la Subdirección de Tecnologías de la Información y Comunicaciones recomienda encarecidamente aplicar los siguientes pasos, con el fin de evitar la exposición a ataques externos y la toma de control de los sistemas:

Mitigación

1º. Solución a las vulnerabilidades:

- **Actualizar** inmediatamente OpenSSL en sistemas o en aplicaciones **a la versión 3.0.7.**

Referencias

- CVE-2022-3786 and CVE-2022-3602: X.509 Email Address Buffer Overflows
- 509 Email Address 4-byte Buffer Overflow (CVE-2022-3602)
- Overview of software (un)affected by vulnerability
- OpenSSL Releases Security Update
- OpenSSL 3.0.0 to 3.0.6 decodes some punycode email addresses in X.509 certificates improperly

---

En caso de haber detectado la explotación de estas vulnerabilidades :

debe reportar el incidente mediante correo electrónico a ayudadigital.sspa@juntadeandalucia.es in dicando en el *Asunto: [Compromiso OpenSSL0711]*

Para cualquier otra duda o consulta al respecto, puede ponerse en contacto con ustic.stic.sspa@juntadeandalucia.es.

Gracias por vuestra atención.

Unidad de Seguridad TIC

Subdirección de Tecnologías de la Información y Comunicaciones

Servicio Andaluz de Salud