Boletin de Seguridad UNAM-CERT-2014-004 Vulnerabilidad Heartbleed en OpenSSL

Una vulnerabilidad en OpenSSL podría permitir la exposición de datos sensibles, incluyendo credenciales de usuario y llaves privadas, debido a un manejo inadecuado de memoria en la extensión heartbeat de TLS.

- **Fecha de Liberación:** 8-Abr-2014
- **Ultima Revisión:** 25-Abr-2014
- **Fuente:** OpenSSL.org
- **CVE ID:** CVE-2014-0160
- **Riesgo** Crítico
- **Problema de Vulnerabilidad** Remoto
- **Tipo de Vulnerabilidad** Divulgación de información

Sistemas Afectados

OpenSSL >= 1.0.1
OpenSSL <= 1.0.1f
OpenSSL == 1.0.2-beta

1. Descripción

Las versiones 1.0.1 a 1.0.1f de OpenSSL tienen una falla en su implementación de la funcionalidad heartbeat de TLS/DTLS, la cual permite a un atacante tener acceso a la memoria privada de alguna aplicación que utilice la biblioteca vulnerable de OpenSSL tomando bloques de 64k. El atacante podría utilizar la vulnerabilidad tantas veces como fuera necesario para obtener información sensible, entre la que podría incluirse:

- Llaves privadas
- Nombres de usuario y contraseñas
- Otros datos sensibles utilizados en los servicios que utilicen la biblioteca vulnerable de OpenSSL

Es importante tener en cuenta que OpenSSL se utiliza en diversos servicios como mecanismo para cifrar el medio de comunicación, por ejemplo:

- Web (https)
- Correo electrónico (imaps, pops, smtps)
- Servicios de directorio (ldaps)
- Redes Privadas Virtuales (VPN)

Este fallo afecta a cualquier software que haga uso de una biblioteca vulnerable de OpenSSL y no deja rastro en las bitácoras de las aplicaciones afectadas debido a que el ataque se establece inmediatamente después de inicializar la transmisión con TLS.

Existen exploits y pruebas de concepto disponibles en Internet que verifican si el servicio es vulnerable y realizan el volcado de la información obtenida.

2. Impacto

Esta falla permite a un atacante acceder desde un sitio remoto a memoria privada de una aplicación que utiliza la biblioteca OpenSSL vulnerable en bloques de 64k.

3. Solución

- Actualizar a la versión OpenSSL 1.0.1g que corrige este vulnerabilidad. Todas las llaves generadas con una versión vulnerable de OpenSSL deberían considerarse comprometidas, por lo que deberían ser generadas e instaladas nuevamente, una vez que el parche haya sido aplicado.
- Verificar con el fabricante del sistema operativo para revisar si existe un paquete que contenga la versión actualizada.
- Recompilar los binarios y bibliotecas de OpenSSL con la opción **-D*OPENSSL_NO_HEARTBEATS*** para no incluir la funcionalidad afectada.
- Se recomienda considerar la implementación de *Perfect Forward Secrecy* para mitigar el daño que podría provocar la revelación de llaves privadas.

4. Verificación

Herramientas de verificación via web

- http://diagnostico.seguridad.unam.mx/check/heartbleed.pl
- http://check.ssltool.com/
- https://filippo.io/Heartbleed/
- http://possible.lv/tools/hb/
- http://rehmann.co/projects/heartbeat/

Herramientas de verificación por línea de comandos

- http://tools.seguridad.unam.mx/heartbleed/
- http://s3.jspenguin.org/ssltest.py
- http://rehmann.co/projects/heartbeat/ssltest.py
- http://foxitsecurity.files.wordpress.com/2014/04/fox_heartbleedtest.zip
- https://github.com/FiloSottile/Heartbleed

Reglas de SNORT para detectar el ataque (SIDs 30510 - 30517)

- http://vrt-blog.snort.org/2014/04/heartbleed-memory-disclosure-upgrade.html

5. Referencias

- The Heartbleed Bug - http://heartbleed.com/
- OpenSSL Security Advisory - https://www.openssl.org/news/secadv_20140407.txt
- US CERT Vulnerability Note VU#720951 - http://www.kb.cert.org/vuls/id/720951
- CERT FI - Security Advisory - https://www.cert.fi/en/reports/2014/vulnerability788210.html
- CERT Australia - Security Advisory - https://www.cert.at/warnings/all/20140408.html
- CIRT Luxembourg - Security Advisory - http://www.circl.lu/pub/tr-21/
- CloudFlare Security Advisory - http://blog.cloudflare.com/staying-ahead-of-openssl-vulnerabilities
- FreshPorts Mailing List - http://www.freshports.org/security/openssl/
- Tor Project Blog - https://blog.torproject.org/blog/openssl-bug-cve-2014-0160
- Debian Security Advisory DSA-2896-1 - https://www.debian.org/security/2014/dsa-2896
- Ubuntu Security Notice USN-2165-1 - http://www.ubuntu.com/usn/usn-2165-1/
- RedHat Security Advisory RHSA-2014:0376-1 - https://rhn.redhat.com/errata/RHSA-2014-0376.html
- Fedora Project Mailing List - https://lists.fedoraproject.org/pipermail/announce/2014-April/003205.html

La Subdirección de Seguridad de la Información/UNAM-CERT agradece el apoyo en la elaboración ó traducción y revisión de éste Documento a:

- Andrés Leonardo Hernández Bermúdez (ahernandez at seguridad dot unam dot mx)
- Ruben Aquino Luna (raquino at seguridad dot unam dot mx)

UNAM-CERT
Equipo de Respuesta a Incidentes UNAM
Subdirección de Seguridad de la Información

incidentes at seguridad.unam.mx
phishing at seguridad.unam.mx
http://www.cert.org.mx
http://www.seguridad.unam.mx
ftp://ftp.seguridad.unam.mx
Tel: 56 22 81 69
Fax: 56 22 80 47