BOLETÍN DE ALERTA

Boletín Nro.: 2015-02
Fecha de publicación: 06/03/2015
Tema: Vulnerabilidad POODLE en SSLv3.0 y su explotación

Sistemas afectados:
Todos los sistemas y aplicaciones que utilizan el protocolo *Secure Socket Layer* (SSL) 3.0 con encadenamiento de cifrado de bloque (CBC) pueden ser vulnerables. Sin embargo, el ataque POODLE (*Padding Oracle On Degradado Legado Encryption*) explota esta vulnerabilidad a través de los navegadores web y servidores web, que es uno de los vectores de ataque más probables.

Algunas implementaciones de TLS (*Transport Layer Security*) también son vulnerables al ataque POODLE.

Descripción:
SSL 3.0 fue la última revisión del protocolo de comunicación seguro SSL ("*Secure Sockets Layers"*) antes de su evolución a lo que hoy se denomina TLS. Su función principal es permitir el envío de claves de cifrado entre aquellas aplicaciones que lo implementen, de manera que se establezca entre ellas una conexión segura que no pueda ser espiada.
Por ejemplo, al conectarse a un sitio web de un banco, para realizar operaciones *online*, lo normal es que el navegador solicite una conexión segura al sitio web de la entidad. De esa forma, la información que se intercambia en esta comunicación está cifrada.
Actualmente, la mayoría de aplicaciones (especialmente los navegadores *web*) están configuradas para utilizar SSL y TLS para esta comunicación segura.
La vulnerabilidad en SSL 3.0, que fue descubierta por los investigadores de Google, consiste en aprovecharse de una característica que hace que, cuando un intento de conexión segura falla, se proceda a intentar realizar de nuevo esa conexión pero con un protocolo de comunicación más antiguo (conocido como *Fallback* o *Downgrade Dance*). De esa forma, un atacante podría ocasionar intencionalmente errores de conexión en protocolos seguros como TLS 1.2, 1.1 y 1.0 y forzar así el uso de SSL 3.0 para aprovechar la vulnerabilidad.
Aunque SSL 3.0 es un estándar de cifrado obsoleto y ha sido reemplazado por TLS, la mayoría de las implementaciones siguen siendo compatibles con SSL 3.0 para interoperar con sistemas y navegadores antiguos, como por ejemplo, Internet Explorer 6. Incluso si un cliente y el servidor

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

soportan una versión de TLS, la mayoría de las implementaciones de SSL/TLS permite la negociación de versión inferiores.

Nótese que POODLE no está orientado a comprometer el sistema, sino a obtener la información que debería viajar cifrada.

Como vemos, es un ataque en dos tiempos. Primero se fuerza el uso de un protocolo no seguro y luego se aprovecha una vulnerabilidad en él. No obstante, para poder realizar este ataque se han de cumplir dos condiciones:

1. El atacante debe ser capaz de controlar una parte de la conexión SSL del lado cliente,
2. El atacante debe tener visibilidad del texto cifrado resultante.

Un escenario común sería cuando el atacante está conectado a la misma red que la víctima, a través de un ataque *Man In The Middle*.

Impacto:

El ataque POODLE puede ser utilizado en contra de cualquier sistema o aplicación que soporte SSL 3.0 con cifrado modo CBC. Esto afecta principalmente a los navegadores y sitios web , pero también incluye cualquier software que utilice librerías SSL/TLS vulnerables (por ejemplo OpenSSL).

Se puede utilizar Poodle para realizar una amplia variedad de ataques, pero el más llamativo y que más puede afectar a la mayor cantidad es la de explotación en escenarios basados en web, pudiendo obtener acceso a los datos sensibles enviados dentro de la sesión web cifrada, como contraseñas, *cookies* y otros *tokens* de autenticación que luego pueden ser utilizados para obtener acceso más completo a un sitio web (robo de identidad de usuario, acceso a los contenidos de bases de datos, etc.). El robo de *cookies* de sesión permite a un atacante realizar acciones tales como registrarse en la cuenta de cualquier servicio *online* (correo, redes sociales, banca), enviar correos en nombre de la víctima, realizar transferencias bancarias, etc. sin necesidad de obtener previamente usuario y contraseña.

Detección:

Existen numerosas herramientas online para detectar si un servidor es vulnerable a POODLE:

- https://www.ssllabs.com/ssltest/
- https://www.poodlescan.com/
- https://pentest-tools.com/vulnerability-scanning/ssl-poodle-scanner
- https://www.tinfoilsecurity.com/poodle

Herramientas para determinar si el navegador es vulnerable:

- https://www.ssllabs.com/ssltest/viewMyClient.html
- https://www.poodletest.com/

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

Solución:
Actualmente no existe una solución para la vulnerabilidad que afecta a SSL 3.0, debido a que la misma constituye una parte esencial del protocolo. Sin embargo, como se trata de una versión antigua, de más de 15 años y que se considera obsoleta, la solución al ataque POODLE consiste en dejar de utilizar SSL 3.0 y todas sus versiones anteriores y usar solo TLS 1.0 y posteriores. De esta forma no se podría forzar que tanto el cliente como el servidor utilicen una versión insegura del protocolo.

La mayoría de los fabricantes brindan guías y/o herramientas para deshabilitar SSL 3.0 en sus productos:

- Red Hat: https://access.redhat.com/articles/1232123
- Mozilla –Firefox: https://addons.mozilla.org/en-US/firefox/addon/ssl-version-control/
- Misceláneas: http://askubuntu.com/questions/537196/how-do-i-patch-workaround-sslv3-poodle-vulnerability-cve-2014-3566
- Zimbra: http://wiki.zimbra.com/wiki/How_to_disable_SSLv3

Algunos investigadores han desarrollado soluciones para una de las condiciones previas; TLS_FALLBACK_SCSV, que es una extensión de protocolo que evita que un atacantes pueda forzar la degradación del protocolo (*downgrade*). OpenSSL ha añadido soporte para TLS_FALLBACK_SCSV a sus últimas versiones; se recomienda las siguientes actualizaciones:

- **OpenSSL 1.0.1**: los usuarios deben actualizar a 1.0.1j.
- **OpenSSL 1.0.0**: los usuarios deben actualizar a 1.0.0o.
- **OpenSSL 0.9.8**: los usuarios deben actualizar a 0.9.8zc.

Tanto cliente como servidor deben soportar TLS_FALLBACK_SCSV para prevenir los ataques de *fallback*.
También se ha descubierto una variante de esta vulnerabilidad que afecta a TLS, por lo que se recomienda aplicar las actualizaciones.

Información adicional:

- https://www.openssl.org/~bodo/ssl-poodle.pdf
- http://www.kb.cert.org/vuls/id/577193
- http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3566
- http://www.welivesecurity.com/la-es/2014/10/15/poodle-vulnerabilidad-ssl-3/
- https://www.imperialviolet.org/2014/12/08/poodleagain.html

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py