Subdirección de Seguridad de la Información - UNAM-CERT -- DGTIC-UNAM

Boletin de Seguridad UNAM-CERT-2014-010 Ataque POODLE y Vulnerablidad al protocolo SSL 3.0 Protocol

Todos los sistemas y aplicaciones que utilizan el protocolo Secure Socket Layer (SSL) 3.0 con cifrado de bloque de encadenamiento (CBC) como modo de cifrado, pueden ser vulnerables. Sin embargo, el ataque POODLE (Padding Oracle On Downgraded Legacy Encryption) demuestra esta vulnerabilidad mediante navegadores y servidores web, que es uno de los escenarios más probables de explotación.

- **Fecha de Liberación:** 17-Oct-2014
- **Ultima Revisión:** 20-Oct-2014
- **Fuente:** https://www.us-cert.gov/ncas/alerts/TA14-290A
- **Riesgo** Moderado
- **Problema de Vulnerabilidad** Local y remoto
- **Tipo de Vulnerabilidad** Ejecución Remota de Código

Sistemas Afectados

SSL == 3.0

1. Descripción

La vulnerabilidad SSL 3,0 deriva de la forma en que los bloques de datos son cifrados bajo un tipo específico de algoritmo de cifrado dentro del protocolo SSL. El ataque POODLE se aprovecha de la función de negociación de la versión de protocolo integrado en SSL / TLS para forzar el uso de SSL 3.0 y aprovechar esta nueva vulnerabilidad para descifrar contenido seleccionado dentro de la sesión SSL. El descifrado se realiza byte a byte y generará un gran número de conexiones entre el cliente y el servidor.

Mientras que SSL 3.0 es un estándar de cifrado viejo y por lo general ha sido reemplazado por Transport Layer Security (TLS) (que no es vulnerable en este sentido), la mayoría de implementaciones SSL / TLS siguen siendo compatibles con SSL 3.0 para interoperar con los sistemas heredados en el interés de una experiencia de usuario sin problemas. Incluso si un cliente y el servidor soportan una versión de TLS, el protocolo SSL / TLS permite la negociación de la versión del protocolo (que se conoce como la " downgrade dance" en otros informes).

El ataque POODLE aprovecha el hecho de que cuando falla un intento de conexión segura, los servidores intentan de nuevo con los protocolos más antiguos, como SSL 3.0. Un atacante que puede desencadenar un fallo de conexión a continuación, puede forzar el uso de SSL 3.0 y tratar el nuevo ataque. Otras dos condiciones se deben cumplir para ejecutar con éxito el ataque POODLE:

1) el atacante debe ser capaz de controlar las porciones del lado del cliente de la conexión SSL (variación de la longitud de la entrada) y
2) el atacante debe tener visibilidad del texto cifrado resultante.

La forma más común de lograr estas condiciones sería actuar como hombre-en-el-medio (MITM), lo que requiere una forma separada todo de ataque para establecer ese nivel de acceso.

2. Impacto

El ataque POODLE puede ser utilizado en contra de cualquier sistema o aplicación que soporte SSL 3.0 con sistemas de cifrado de modo CBC. Esto afecta a los navegadores y sitios web más actuales, pero también incluye cualquier software que, o bien las referencias a SSL vulnerables / biblioteca TLS (por ejemplo OpenSSL) o implementa el SSL / TLS propio conjunto de protocolos. Mediante la explotación de esta vulnerabilidad en un escenario basado en la web probablemente, un atacante puede obtener acceso a los datos sensibles aprobadas dentro de la sesión web cifrada, tales como contraseñas, cookies y otros tokens de autenticación que luego se pueden utilizar para obtener acceso más completo a un sitio web (hacerse pasar por ese usuario, acceder a los contenidos de bases de datos, etc).

3. Solución

Actualmente no existe una solución para la vulnerabilidad SSL 3.0 en sí, ya que el tema es fundamental para el protocolo; Sin embargo, deshabilitando el soporte en las configuraciones de SSL 3.0 en el sistema y aplicación es la solución más viable. Algunos de los mismos investigadores que descubrieron la vulnerabilidad también han desarrollado una solución para una de las condiciones previas; TLS_FALLBACK_SCSV es una extensión del protocolo que evita que los atacantes MITM sean capaces de forzar el uso de versiones anteriores. OpenSSL ha añadido soporte para TLS_FALLBACK_SCSV a sus últimas versiones y recomienda las siguientes actualizaciones:

OpenSSL 1.0.1 usuarios deben actualizar a 1.0.1j.

OpenSSL 1.0.0 usuarios deben actualizar a 1.0.0o.

OpenSSL 0.9.8 usuarios deben actualizar a 0.9.8zc.

Ambos, clientes y servidores necesitan soportar TLS_FALLBACK_SCSV para prevenir los ataques de downgrade. Otras implementaciones de SSL 3.0 probablemente también estén afectadas por POODLE. Comuníquese con su proveedor para obtener más detalles. Información adicional de productos puede estar disponible en National Vulnerability Database (NVD) para CVE-2.014-3566 [3] o en Vulnerabilidades de CERT VU # 577193.

4. Referencias

[1] This Poodle Bites: Exploiting The SSL Fallback
[2] OpenSSL Security Advisory [15 Oct 2014]
[3] Vulnerability Summary for CVE-2014-3566
[4] CERT Vulnerability Note VU#577193

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

- José Roberto Sánchez Soledad (rsanchez 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