La Vulnerabilidad SSL POODLE, Ahora Ataca La Seguridad Del Protocolo TLS

POODLE, una falla critica de SSL descubierta en octubre que fue parcheado y solucionada por los webmasters de todo el mundo después de que Google alertó sobre este fallo de seguridad, ha hecho de nuevo noticia y esta vez la vulnerabilidad afecta a las implementaciones del protocolo más reciente, el Transport Layer Security (TLS).

La grave ***vulnerabilidad POODLE*** que afectó al protocolo de encriptación web más utilizado (SSL), ha vuelto una vez más y es probable que afecte a algunos de los sitios web más populares del mundo, incluidos los de propiedad u operados por Bank of America, el US Department of Veteran's Affairs, y Accenture.

El fallo ***POODLE (Padding Oracle On Downgraded Legacy Encryption)***, revelada hace dos meses por el equipo de seguridad de Google, permite a los atacantes realizar el famoso ataque Man-in-the-Middle (MitM) con el fin de **interceptar el tráfico entre el navegador del usuario y un sitio web HTTPS** para descifrar información sensible, como las cookies de autenticación del usuario.

Ahora, el fallo peligroso se ha usado en algunas versiones de TLS, el aparente sucesor seguro de SSL. La nueva vulnerabilidad (***CVE-2.014-8.730***) afecta la versión 1.2 del protocolo TLS. Los investigadores de la *firma de seguridad Qualys* dice, «algunas implementaciones TLS omiten la comprobación de la estructura de relleno después del descifrado.»

«El impacto de este problema es similar a la del POODLE, este ataque es un poco más fácil de ejecutar, sin necesidad de rebajar los clientes modernos a SSL 3, TLS 1.2 lo hará muy bien», ha dicho Ivan Ristic, director de seguridad de Qualys, el cual escribió en un post titulado POODLE bites TLS.

Qualys ha proporcionado una prueba gratuita, Test SSL Server, que mostró algunos de los sitios web más importantes del Internet incluyendo ***Bank of America***, VMware, el Departamento de Asuntos de Veteranos de Estados Unidos, y consultoría de negocios Accenture, se ven afectadas por el bug. La vulnerabilidad es muy grave como el análisis más reciente de SSL Pulse mostró que alrededor del 10 por ciento de los servidores son vulnerables al **ataque POODLE a través de TLS**.

Los administradores de sitios web que deseen comprobar si sus servidores son vulnerables al ataque POODLE recién descubierto a través de TLS, puede usar la prueba del servidor SSL Qualys Labs, que ha sido actualizada en su página web con el fin de detectar el problema .