Descubierto Grave Fallo De Seguridad En OAuth y OpenID

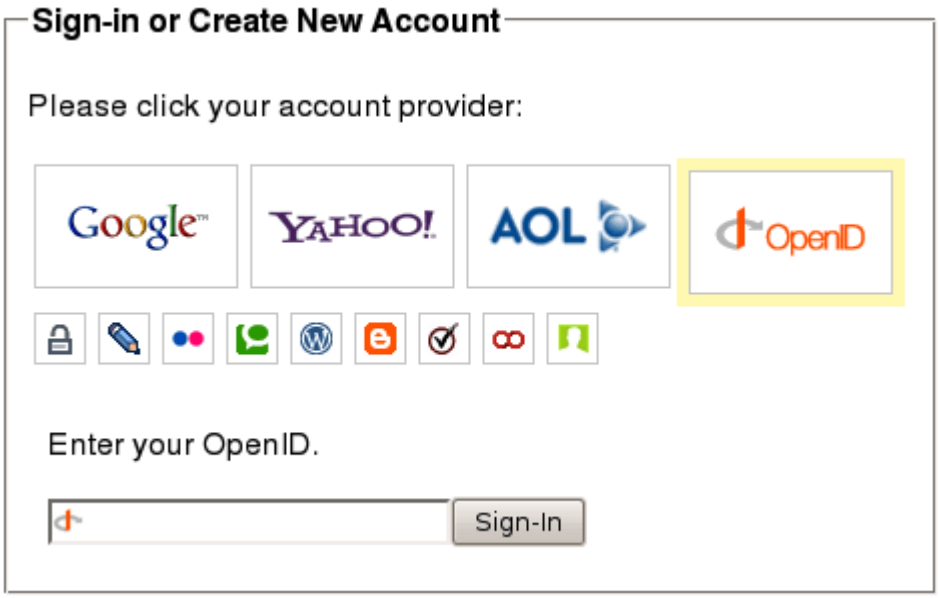
Siguiendo los pasos de la vulnerabilidad de OpenSSL conocida como Heartbleed , otra gran falla ha sido encontrada en el popular software de seguridad de código abierto. Esta vez, los agujeros se han encontrado en las herramientas de autentificacion OAuth y OpenID , utilizado por una gran cantidad de sitios web y gigantes de la tecnología como Google, Facebook, Microsoft , y LinkedIn, entre otros.

Wang Jing, estudiante de doctorado en la **Universidad Tecnológica de Nanyang en Singapur**, descubrió que el fallo de seguridad nombrado como «**Covert Redirect**«, se puede utilizar para hacer pasar una ventana emergente como el login en el dominio de un sitio afectado. **Covert Redirect** se basa en un parámetro de un **exploit reconocido**.

Por ejemplo, alguien hace clic en un enlace malicioso de **phishing** saldrá una ventana emergente en Facebook, pidiéndoles que se autorice la aplicación. En lugar de utilizar un nombre de dominio falso que es similar a engañar a los usuarios, la vulnerabilidad **Covert Redirect** utiliza la dirección de un **sitio real para la autenticación**.

Si un usuario decide autorizar el inicio de sesión , los datos personales (en función de lo que se está pidiendo) se darán a conocer al atacante en vez del sitio web legítimo. Esto puede ir desde direcciones de correo electrónico , fechas de nacimiento , listas de contactos y el control , posiblemente, incluso de la cuenta.

Independientemente de si la víctima decide autorizar la aplicación, que a continuación se redirecciona a un sitio web de la elección del atacante , lo que podría comprometer aún más a la víctima.



Wang dice que ya ha contactado con Facebook y se ha informado de la falla, pero esta le respondio: «la empresa entiende los riesgos asociados con OAuth 2.0,» y que «lejos de obligar a cada aplicación en la plataforma para utilizar una lista blanca», la solucion de este error era «algo que no se puede lograr en el corto plazo.»

Facebook no es el único lugar afectado. Wang dice que ha informado de esto a Google, LinkedIn y Microsoft, que le dio varias respuestas sobre cómo manejarían el asunto.

Los usuarios que desean evitar cualquier pérdida potencial de datos deben tener cuidado al hacer clic en enlaces que piden inmediatamente que inicie sesión en Facebook o Google . Al cerrar la ficha de inmediato, evitará cualquier ataque de redirección .

Si bien este problema no es tan grave como Heartbleed , es relativamente fácil de hacer, por lo menos hasta que sea parcheado, que según **Wang**, es bastante difícil de implementar debido a que los sitios de terceros tienen «pocos incentivos» para solucionar el problema . El costo es un factor, así como también el punto de vista de la compañía (como Facebook), ya que tienen la responsabilidad de hacer caer en cuenta la

gravedad de los ataques.