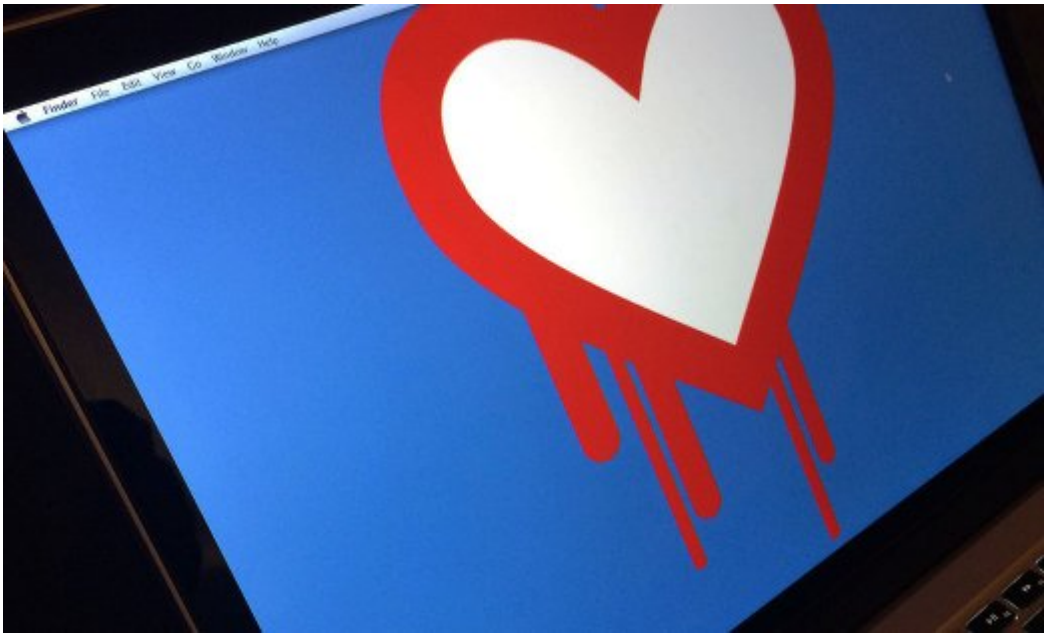
El Equipo De Node.js Aceptó El Reto De CloudFlare Exponiendo Las Claves SSL

Fedor Indutny, un miembro clave del equipo de **Node.js**, ha demostrado que es de hecho posible para un atacante **sniffear** las **claves SSL privado** de servidor expuesto por el **bug Heartbleed**. La prueba fue en respuesta a un reto que propuso **CloudFlare**, en el cual pidió a la comunidad de seguridad informática tomar las llaves de un servidor de demostración.



La noticia sobre el bug de **Heartbleed** sacudió el mundo de la tecnología a principios de esta semana. El error, un error inocuo en el protocolo de «**heartbeat**«, del protocolo **estándar del SSL**, durante años había puesto la mayor parte de la **Web en riesgo** de tener las expuestas las claves de cifrado, contraseñas y otros datos sensibles. Para empeorar las cosas, el **exploit** es prácticamente indetectable, lo que hace difícil de saber si los atacantes ya habían descubierto el error y se han aprovechado de ella.

CloudFlare creó el reto después de que su propio equipo no tuvo éxito en exponer las claves de sus propios servidores. La compañía planteo el viernes bien temprano, que el **uso de Heartbleed para conseguir las claves privadas** es «algo difícil … de hecho puede ser imposible.»

Desafortunadamente, la compañía de **CloudFlare** se ha equivocado al decir esto. Explotar las claves privadas no toma demasiado tiempo, como lo afirma **Indutny**, ya que su equipo tomó tan sólo tres horas para localizar la **clave privada de SSL**.

CloudFlare se ha comprometido en proporcionar detalles sobre cómo **Indutny** obtuvo las llaves, pero es probable que ninguna de las partes revele el método exacto inmediatamente, con el fin de proporcionar a los administradores más tiempo para cambiar sus credenciales SSL. **Mateo Prince**, CEO de **CloudFlare** mencionó que sospecha que las llaves se filtraron cuando el equipo reinició el servidor del reto.

Solo queda esperar, que llegue la información de como se obtuvieron estas claves en tan poco tiempo, a los servidores y desarrolladores encargados de solucionar este problema, mientras tanto, solo queda usar encriptadores de contraseñas ó administradores de estas para fortalecer la seguridad de nuestras cuentas.