HFC - Web Hacking Dicter Tadeo Garcia Rosas
Tarea 1 - Heartbleed

¿Qué es Heartbleed?

Heartbleed es una vulnerabilidad en un software de código abierto llamado openssl el cual es una implementación del protocolo de red TLS de la capa de transporte, dicho protocolo es importante ya que provee autenticación, integridad y confidencialidad en la comunicación de redes, por ejemplo cuando visitamos un sitio web y TLS nos ayuda a verificar la identidad del servidor, establecer una conexión cifrada y enviar datos a través de dicha conexión.

TLS nos indica cómo es que se realiza el intercambio de información entre dos puntos finales de una red, podríamos pensarlos como un servidor y un cliente, a grandes rasgos un intercambio de información en TLS tiene dos fases:

- En la primera el cliente y el servidor establecen los algoritmos de cifrado y los parámetros del intercambio de información, en esta fase los mensajes van en texto claro.
- En la segunda fase una vez acordado el algoritmo se hace el intercambio de información de forma cifrada.

Dentro de la versión 1.2 de TLS se introdujo el concepto de heartbeat con el cual se esperaba poder tener una forma de comprobar la conexión con el otro endpoint de la red, la forma en la que funciona este concepto es mediante el envío de un mensaje “heartbeat” desde un lado de la red y se responde con ese mismo mensaje “heartbeat” desde el otro lado de la comunicación.

La composición de este mensaje es de 2 campos: la longitud del mensaje y la carga o payload del mensaje que por lo general es una cadena, la respuesta a este envío de mensaje debe ser exactamente de la misma longitud y el contenido/payload debe ser el mismo. La vulnerabilidad en openssl consta de no verificar que la longitud del mensaje en la petición, es decir cuando se envía, pues si la solicitud miente sobre su longitud y en el cuerpo de la petición no envía nada o envia un cuerpo con una longitud menor a la declarada, el otro endpoint termina devolviendo una petición con la longitud solicitada la cual va a incluir un segmento de memoria, es decir una fuga de información la cual podría contener información sensible como credenciales usadas recientemente, llaves criptográficas, etc.

Como parte importante de la vulnerabilidad, la implementación inicial de TLS permite que las peticiones y las respuestas se enviaran en texto claro, es decir en la primera fase del protocolo.