Mostafa Fatayri

202101056

Heartbleed bug was a vulnerability in the OpenSSL cryptographic software library, which allowed attackers to steal data protected by the SSL/TLS encryption used to secure the internet. This bug resides in the implementation of the heartbeat extension for the transport layer Security (TLS ) protocol. As soon as a client sends a heartbeat request to a server, it will include a payload and the wight of the payload. The response of the server will be echoing back the payload. Due to a missing bounds check in the implementation of OpenSSL , any attacker could lie about the size of the payload, which will trick the server into responding with a payload followed by 64 KB of server memory. This data could include some confidential data like usernames , password or even encryption keys that will decrypt messages. It was called Heartbleed because this vulnerability was in the “heartbeat” extension of the OpenSSL library and it was a major issue in bleeding information from the memory .It was discovered by a team of security engineers ( Riku, Antti, and Matti ) at Condenomicon and Neel Mehta of Google Security in April 2014. After the Vulnerability was discovered , a fixed version of OpenSSL was released on April 7 2014 and OpenSSL remined usable but vulnerable versions needed to be updated to the patched version and some systems had to regenerate their cryptographic keys and SSL certificates adding some reinforcement for the users to change passwords.

Reference :

Video 1 : <https://youtu.be/eCGKf1XD-ME?si=Vrcr2gLVpBRd7GqJ>

Video 2 : <https://youtu.be/SgJm0C6jzbo?si=oKsJ3H6ctWmIbypw>