Heartbleed Bug

- Timetable
  - Existed since December 31, 2011
  - Discovered April 1, 2014
  - Fixed April 7, 2014
- Nature of the Flaw
  - Affects several versions of OpenSSL, which is software used for SSL and TLS encryption
  - Can be exploited to cause a website to leak private data
    - Passwords and other sensitive customer data
    - Security certificates, which allow the attacker to decrypt traffic
  - Many websites are apparently still vulnerable
  - Operating systems are also affected: Linux, Mac OS X, BSD, Android
  - Some applications are affected: LibreOffice, LogMeIn, Filemaker
  - No one knows if the bug has been exploited during the past two years
- Remediation
  - Website administrators are advised to update OpenSSL and reissue security certificates
  - End Users
    - Update their OS: Linux, BSD, Android 4.1.1
    - Update their applications
    - Change their passwords for affected websites
- More information:
  - What is Heartbleed
    - http://www.pcworld.com/article/2140920/heartbleed-bug-in-openssl-puts-encrypted-communications-at-risk.html
    - http://www.pcworld.com/article/2153303/one-month-later-hundreds-of-thousands-of-servers-still-vulnerable-to-heartbleed.html
    - http://heartbleed.com/
    - http://en.wikipedia.org/wiki/Heartbleed
  - Who is affected
    - http://mashable.com/2014/04/09/heartbleed-bug-websites-affected/
    - http://en.wikipedia.org/wiki/Heartbleed#Impact