DATA AND NETWORK SECURITY

Case Study III: Heartbleed

Website: heartbleed.com

1

Overview

- Classification: Vulnerability
  - Severity: High
  - Timeframe: 2014
- Product:
  - OpenSSL [freeware implementation of Secure Socket Layer]
  - Versions: 1.0.1 -> 1.0.1f
  - Patched: 1.0.1g and forward

2

Vulnerability

- SSL includes a 'heartbeat' message/'heartbeat' response.
  - Normally, client sends a short buffer and asks for it back
  - Crafted heartbeat messages can send short buffer but 'lie' about size of buffer'
    - Send 'bird'
    - Ask server to echo 500 byte word: 'bird'
    - No length check/verification of client heartbeat packet by OpenSSL
    - Returned data includes data following it on the stack

3

4

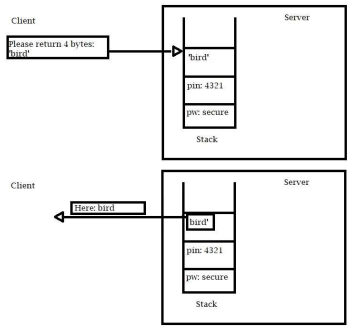
Discovery and Public Release

- Discovered by Google and Codenomicon
- Google quietly shared with OpenSSL developers
- Codenomicon named it 'Heartbleed'
  - set up a website,
  - released information publicly
  - Purpose: Public awareness and to force imminent action (patching)

4

5

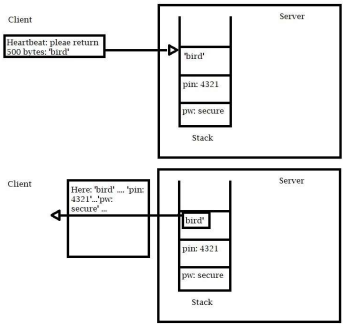
Vulnerability



5

6

Vulnerability



6

7

Impact

- Data on stack can include:
  - Other user cookies
  - Passwords
  - Encryption keys
  - Data that can allow impersonation of other users

7

8

Reverse Heartbeat

- Clients also vulnerable [browsers using OpenSSL for SSL/TLS]
  - Malicious server can perform same deception
  - Client can reveal secret data from user's PC including passwords, keys, etc.

8

9

Mitigation

- Build OpenSSL with switch
  - –DOPENSSL_NO_HEARTBEATS
- Install OpenSSL 1.0.1g or later

9

10

5 years later

- Many devices are still unpatched
- Mainly devices which complicate patching or are unable to be patched.

10

11

Sources

- http://heartbleed.com/
- https://blog.malwarebytes.com/exploits-and-vulnerabilities/2019/09/everything-you-need-to-know-about-the-heartbleed-vulnerability/
- https://en.wikipedia.org/wiki/Heartbleed
- https://blog.malwarebytes.com/exploits-and-vulnerabilities/2019/09/everything-you-need-to-know-about-the-heartbleed-vulnerability/

11