

## [อัปเดต Ubuntu Precise 12.04 นี้ Heartbleed](#) [1]

เขียนโดย [sake](#) [2] เมื่อ 2014-04-09 17:32



วงการ admin สะเทือน งานเข้ากันเต็มๆ เมื่อ ssl library ยอดฮิต อย่าง openssl เป็นเป้า ตาม [Heartbleed attack](#) [3] เลยต้องอัปเดต กัน โดยเฉพาะเครื่องเก่าๆ ส่วนผม มีเครื่องนึงที่เป็น ubuntu precise 12.04 เลยต้องลงมือลงมือกันหน่อย

ที่ทำไม่ได้โรมาก จากการตรวจสอบ พบว่า ตาม USN-2165-1: OpenSSL vulnerabilities <http://www.ubuntu.com/usn/usn-2165-1/> [4] ได้ระบุวิธีไว้แล้ว

Ubuntu 12.04 LTS:

libssl1.0.0 1.0.1-4ubuntu5.12

พอดู เป็นลิงก์ไปยัง source package

เริ่มจาก update source กัน .ให้แน่ใจว่าเปิด repo precise-security/main อยู่ แล้ว

จากนั้นติดตั้ง package ที่จำเป็นในการ build

1. [root@campus](#) [5]:~# apt-get update
2. [root@campus](#) [5]:~# apt-get upgrade
3. [root@campus](#) [5]:~# apt-get install devscripts
4. [root@campus](#) [5]:~# apt-get build-dep openssl
5. [root@campus](#) [5]:~# apt-get source openssl
6. [root@campus](#) [5]:~# apt-get source openssl
7. Reading package lists... Done

8. Building dependency tree
9. Reading state information... Done
10. NOTICE: 'openssl' packaging is maintained in the 'Svn' version control system at:
11. <svn://svn.debian.org/pkg-openssl/openssl/>
12. Need to get 4592 kB of source archives.
13. Get:1 <http://mirror.kku.ac.th/ubuntu/> [6] precise-security/main openssl 1.0.1-4ubuntu5.12 (dsc) [2365 B]
14. Get:2 <http://mirror.kku.ac.th/ubuntu/> [6] precise-security/main openssl 1.0.1-4ubuntu5.12 (tar) [4454 kB]
15. Get:3 <http://mirror.kku.ac.th/ubuntu/> [6] precise-security/main openssl 1.0.1-4ubuntu5.12 (diff) [136 kB]
16. Fetched 4592 kB in 0s (27.9 MB/s)
17. gpgv: Signature made Tue Apr 8 03:19:33 2014 ICT using RSA key ID A744BE93
18. gpgv: Can't check signature: public key not found
19. dpkg-source: warning: failed to verify signature on ./openssl\_1.0.1-4ubuntu5.12.dsc
20. dpkg-source: info: extracting openssl in openssl-1.0.1
21. dpkg-source: info: unpacking openssl\_1.0.1.orig.tar.gz
22. dpkg-source: info: unpacking openssl\_1.0.1-4ubuntu5.12.debian.tar.gz
23. dpkg-source: info: applying ca.patch
24. dpkg-source: info: applying config-hurd.patch
25. dpkg-source: info: applying debian-targets.patch
26. dpkg-source: info: applying engines-path.patch
27. dpkg-source: info: applying make-targets.patch
28. dpkg-source: info: applying man-dir.patch
29. dpkg-source: info: applying man-section.patch
30. dpkg-source: info: applying no-rpath.patch
31. dpkg-source: info: applying no-symbolic.patch
32. dpkg-source: info: applying pic.patch

33. dpkg-source: info: applying valgrind.patch
34. dpkg-source: info: applying rehash-crt.patch
35. dpkg-source: info: applying rehash\_pod.patch
36. dpkg-source: info: applying shared-lib-ext.patch
37. dpkg-source: info: applying stddev.patch
38. dpkg-source: info: applying version-script.patch
39. dpkg-source: info: applying gnu\_source.patch
40. dpkg-source: info: applying c\_rehash-compat.patch
41. dpkg-source: info: applying libdoc-manpgs-pod-spell.patch
42. dpkg-source: info: applying libssl-misspell.patch
43. dpkg-source: info: applying openssl-pod-misspell.patch
44. dpkg-source: info: applying pod\_req\_misspell2.patch
45. dpkg-source: info: applying pod\_pksc12.misspell.patch
46. dpkg-source: info: applying pod\_s\_server.misspell.patch
47. dpkg-source: info: applying pod\_x509setflags.misspell.patch
48. dpkg-source: info: applying pod\_ec.misspell.patch
49. dpkg-source: info: applying pkcs12-doc.patch
50. dpkg-source: info: applying dgst\_hmac.patch
51. dpkg-source: info: applying block\_diginotar.patch
52. dpkg-source: info: applying block\_digicert\_malaysia.patch
53. dpkg-source: info: applying no\_ssl2.patch
54. dpkg-source: info: applying vpaes.patch
55. dpkg-source: info: applying tls1.2\_client\_algorithms.patch
56. dpkg-source: info: applying perlpath-quilt.patch

57. dpkg-source: info: applying tls12\_workarounds.patch

58. dpkg-source: info: applying ubuntu\_deb676533\_arm\_asm.patch

59. dpkg-source: info: applying CVE-2012-2110.patch

60. dpkg-source: info: applying CVE-2012-2110b.patch

61. dpkg-source: info: applying CVE-2012-2333.patch

62. dpkg-source: info: applying CVE-2012-0884-extra.patch

63. dpkg-source: info: applying lp1018998.patch

64. dpkg-source: info: applying lp1020621.patch

65. dpkg-source: info: applying lp973741.patch

66. dpkg-source: info: applying CVE-2013-0166.patch

67. dpkg-source: info: applying CVE-2013-0169.patch

68. dpkg-source: info: applying fix\_key\_decoding\_deadlock.patch

69. dpkg-source: info: applying openssl-1.0.1e-env-zlib.patch

70. dpkg-source: info: applying CVE-2013-4353.patch

71. dpkg-source: info: applying CVE-2013-6449.patch

72. dpkg-source: info: applying CVE-2013-6450.patch

73. dpkg-source: info: applying no\_default\_rdrand.patch

74. dpkg-source: info: applying CVE-2014-0076.patch

75. dpkg-source: info: applying CVE-2014-0160.patch

76. [root@campus](#) [5]:~# ls

77. openssl-1.0.1                    openssl\_1.0.1.orig.tar.gz

78. openssl\_1.0.1-4ubuntu5.12.debian.tar.gz openssl\_1.0.1-4ubuntu5.12.dsc

79. [root@campus](#) [5]:~# cd openssl-1.0.1/

80. [root@campus](#) [5]:~/openssl-1.0.1# dpkg-buildpackage -us -uc -nc

จากนั้น ระบบจะเริ่ม compile deb package ทั้งหมดที่ได้รับไว้ใน spec file  
เมื่อเสร็จสิ้น จะได้ dpkg เพื่อลงทับอันเก่า

1. `root@campus [5]:~/openssl-1.0.1# cd ..`
2. `root@campus [5]:~# ls`
3. `libssl1.0.0-udeb_1.0.1-4ubuntu5.12_amd64.udeb`
4. `libssl1.0.0_1.0.1-4ubuntu5.12_amd64.deb`
5. `openssl-1.0.1`
6. `openssl_1.0.1-4ubuntu5.12.debian.tar.gz`
7. `openssl_1.0.1-4ubuntu5.12.dsc`
8. `openssl_1.0.1-4ubuntu5.12_amd64.changes`
9. `libcrypto1.0.0-udeb_1.0.1-4ubuntu5.12_amd64.udeb openssl_1.0.1-4ubuntu5.12_amd64.deb`
10. `libssl-dev_1.0.1-4ubuntu5.12_amd64.deb openssl_1.0.1.orig.tar.gz`
11. `libssl-doc_1.0.1-4ubuntu5.12_all.deb libssl1.0.0-dbg_1.0.1-4ubuntu5.12_amd64.deb`
- 12.
13. `root@campus [5]:~# dpkg -i *.deb`
14. (Reading database ... 248296 files and directories currently installed.)
15. Preparing to replace libssl1.0.0 1.0.1-4ubuntu5.12 (using libssl1.0.0\_1.0.1-4ubuntu5.12\_amd64.deb) ...
16. Unpacking replacement libssl1.0.0 ...
17. Selecting previously unselected package libssl1.0.0-dbg.
18. Unpacking libssl1.0.0-dbg (from libssl1.0.0-dbg\_1.0.1-4ubuntu5.12\_amd64.deb) ...
19. Preparing to replace libssl-dev 1.0.1-4ubuntu5.12 (using libssl-dev\_1.0.1-4ubuntu5.12\_amd64.deb) ...
20. Unpacking replacement libssl-dev ...
21. Preparing to replace libssl-doc 1.0.1-4ubuntu5.12 (using libssl-doc\_1.0.1-4ubuntu5.12\_all.deb) ...
22. Unpacking replacement libssl-doc ...

23. Preparing to replace openssl 1.0.1-4ubuntu5.12 (using openssl\_1.0.1-4ubuntu5.12\_amd64.deb) ...
24. Unpacking replacement openssl ...
25. Setting up libssl1.0.0 (1.0.1-4ubuntu5.12) ...
26. locale: Cannot set LC\_CTYPE to default locale: No such file or directory
27. locale: Cannot set LC\_ALL to default locale: No such file or directory
28. Setting up libssl1.0.0-dbg (1.0.1-4ubuntu5.12) ...
29. Setting up libssl-dev (1.0.1-4ubuntu5.12) ...
30. Setting up libssl-doc (1.0.1-4ubuntu5.12) ...
31. Setting up openssl (1.0.1-4ubuntu5.12) ...
32. Processing triggers for man-db ...
33. locale: Cannot set LC\_CTYPE to default locale: No such file or directory
34. locale: Cannot set LC\_ALL to default locale: No such file or directory
35. Processing triggers for libc-bin ...
36. ldconfig deferred processing now taking place
37. [root@campus](#) [5]:~# apt-get -f install
38. Reading package lists... Done
39. Building dependency tree
40. Reading state information... Done
41. 0 upgraded, 0 newly installed, 0 to remove and 2 not upgraded.

ตรวจสอบ version openssl ในระบบ

1. [root@campus](#) [5]:~# dpkg -l | grep openssl

2. ii	openssl	1.0.1-4ubuntu5.12	Secure Socket Layer (SSL) binary and related cryptographic tools
-------	---------	-------------------	--

3. [root@campus](mailto:root@campus) [5]:~#

ทดสอบกับเครื่องมือ



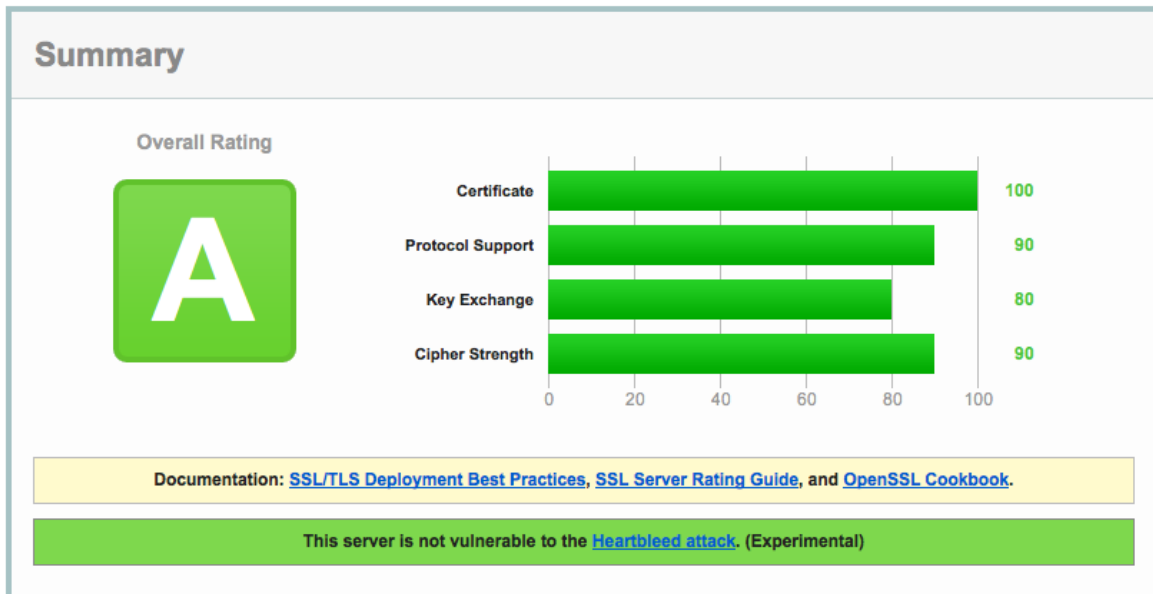
[Home](#) [Projects](#) [Qualys.com](#) [Contact](#)

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > fb.kku.ac.th

## SSL Report: fb.kku.ac.th (202.28.93.209)

Assessed on: Wed Apr 09 08:16:49 UTC 2014 | [Clear cache](#)

[Scan Another »](#)



แค่นี้น่าจะพอไหว :P

Tags: [Ubuntu](#) [7]

[precise](#) [8]

[heartbleed](#) [9]

Source URL (modified on 2015-11-13 06:08): <https://sake.in.th/node/101>

### Links

[1] <https://sake.in.th/blog/%E0%B8%AD%E0%B8%B1%E0%B8%9E%E0%B9%80%E0%B8%94%E0%B8%95UbuntuPrecise12.04%E0%B8%AB%E0%B8%99%E0%B8%B5Heartbleed>

[2] <https://sake.in.th/users/sake>

[3] <http://heartbleed.com>

[4] <http://www.ubuntu.com/usn/usn-2165-1/>

[5] <mailto:root@campus>

[6] <http://mirror.kku.ac.th/ubuntu/>

[7] <https://sake.in.th/category/sitetags/ubuntu>

[8] <https://sake.in.th/tags/sitetags/http%3A/sake.in.th/taxonomy/term/112/edit>

[9] <https://sake.in.th/tags/sitetags/http%3A/sake.in.th/taxonomy/term/113/edit>

