http://www.ositus.com/2014/04/penjelasan-lengkap-tentang-heartbleed.html

http://primonymous.blogspot.com/2014/04/penjelasan-tentang-heartbleed-bug.html

http://tekno-jurnal.blogspot.com/2014/06/pengertian-dancara-mengatasi-heartbleed.htmlPengertian HeartBleed

http://winpoin.com/apa-itu-heartbleed-bagaimana-cara-mengatasinya-dan-kabar-sesat-mengenainya/

http://ekajogja.com/heartbleed-bug-definisi-titik-rentan-dan-cara-penanggulangannya/

**Pengertian HeartBleed**

Internet memiliki set protokol untuk menangani keamanan ketika beroperasi mengalirkan trafik data yang sering disebut sebagai Secure Socket Layer (SSL) dan diteruskan Transport Layer Security (TLS).

Protokol SSL / TLS menjadi bagian utama dari sistem kerja yang ada pada web modern yang menyajikan fungsi keamanan dan privasi di internet bagi sejumlah aplikasi seperti website, email, pesan instan (IM), dan beberapa virtual private networks (VPN).

SSL adalah standar keamanan yang akan mengenkripsi teks (seperti username dan password) yang user kirim via browser.  OpenSSL adalah salah satu teknik SSL tersebut. OpenSSL kemudian dikembangkan secara Open Source untuk membantu proses pengamanan protokol di internet. OpenSSL diterapkan pada akhir tahun 1998 silam .

Heartbleed adalah celah keamanan pada salah satu ekstensi OpenSSL yang disebut heartbeat, yang tujuannya adalah untuk mengecek apakah komputer user masih terhubung ke sebuah server. Celah keamanan memungkinkan attacker untuk membaca memori dari server yang dilindungi oleh OpenSSL. Dengan celah keamanan tersebut para attacker dapat mencuri data penting yang disimpan deserver seperti password, username, dan informasi penting lainnya.

Pembacaan memori sistem ini akan mengungkap kunci-kunci rahasia (secret keys)yang berfungsi untuk:

* mengidentifikasi penyedia layanan
* mengenkripsi lalu lintas data, nama dan password pengguna, juga konten aktual.

Pada akhirnya,attacker bisa:

* mencuri dengar lalu lintas komunikasi
* mencuri data secara langsung dari server dan user
* serta menyamar sebagai penyedia layanan maupun pengguna.

**Awal kemunculan dan Penyebaran heartbleed**

Neel Mehta adalah orang yang menemukan pertama kali heartbleed ,dia salah satu anggota Google Security. Atas jasanya tersebut, dia mendapatkan uang sebesar US$ 15 ribu dari Internet Bug Bounty. Namun oleh Neel, uang itu langsung disumbangkan kepada yayasan The Freedom of Press Foundation yang bergerak di bidang keamanan komunikasi digital.

Seperti yang dijelaskan pada pengertian heartbleed merupakan bug pada ekstensi Heartbeat, maka heartbleed akan muncul ketika heartbeat diimplementasikan di OpenSSL. Ekstensi Heartbeat dibuat oleh Dr. Robin Seggelmann pada tahun 2011. Ekstensi ini kemudian direview oleh Dr. Stephen N. Henson (salah satu dari empat core developer OpenSSL) yang ternyata gagal menyadari adanya bug di ekstensi tersebut. Heartbeat pun akhirnya dijadikan sebagai ekstensi OpenSSL yang aktif secara default dan mulai diadopsi oleh banyak pengelola website sejak dirilisnya OpenSSL versi 1.0.1 pada 14 Maret 2012.

Setidaknya 2/3 website di dunia menggunakan proteksi OpenSSL, sehingga sebanyak itu pula penyebarannya. Website besar seperti Google, Gmail, Facebook, Dropbox, Yahoo, Flickr, Instagram, Pinterest, dan berbagai website populer terkena heartbleed.

**Cara Mengetahui Website yang Terkena Heartbleed**

Dari sisi pengguna :

1. Melakukan pengecekan dengan menggunakan Heartbleed Test dari Filippo ataupun dari McAfee.
2. Masukkan URL website yang ingin dicek.
3. Jika hasilnya vulnerable maka website tersebut masih belum kebal terhadap Heartbleed.
4. Atau dengan menggunakan addon browser untuk semakin memudahkan melihat apakah website yang dikunjungi sudah kebal terhadap Heartbleed atau belum.

Dari sisi pengelola website :

1. Mengecek versi OpenSSL di server yang digunakan.
2. Jika versi OpenSSL di server adalah 1.0.1 hingga 1.0.1f, maka server tersebut belum kebal terhadap Heartbleed.

**Cara Mengatasi Heartbleed**

Bagi pengguna :

Beberapa orang menyarankan untuk segera mengganti password setelah Heartbleed ditemukan. Hal ini salah dan kurang tepat. Jika situs yang digunakan belum kebal terhadap Heartbleed, tunggu hingga pengelola website melakukan patch terhadap OpenSSL di servernya. Setelah situs tersebut kebal terhadap Heartbleed, barulah mengganti password. Mengganti password saat situs tersebut belum kebal terhadap Heartbleed cukup berbahaya. Attacker masih bisa mencuri detail password baru yang dimasukkan. Mereka tidak bisa mengambil detail password baru jika OpenSSL di server situs tersebut sudah dipatch oleh pengelola.

Solusi lainnya adalah dengan menggunakan satu password untuk satu situs. Dengan begitu jika tanpa sengaja menggunakan layanan website yang belum kebal terhadap Heartbleed, dan attacker berhasil mengambil detail akun kamu, maka dia tidak bisa membobol akun kamu di layanan-layanan lainnya. Untuk memudahkan dalam mengingat password, bisa menggunakan Password Manager seperti KeePass maupun LastPass. Untuk semakin mengamankan akun kamu, pastikan untuk mengaktifkan Two-Factor Authentication jika memang fitur tersebut tersedia. Saat ini berbagai situs besar dan populer sudah menerapkan teknologi ini. Dengan begini attacker tidak akan bisa bebas keluar masuk ke akun kamu meskipun sudah mengantongi username dan passwordnya.

Bagi Pengelola Situs :

Jika server masih menggunakan OpenSSL 1.0.1 hingga 1.0.1f, segera update OpenSSL tersebut ke versi 1.01g. Cara mengupdatenya bervariasi tergantung dari OS apa yang digunakan di server. Jangan lupa untuk mengingatkan user untuk mengganti password.

**Beberapa Mitos yang Salah Seputar Heartbleed**

1. Heartbleed itu virus : Salah. Heartbleed bukanlah virus. HeartBleedadalah bug diekstensi Heartbeat OpenSSL versi 1.0.1 sampai 1.0.1f
2. Segera update antivirus biar kebal Heartbleed : Salah. Update antivirus tidak akan berpengaruhterhadap kebal atau tidaknya PC terhadap Heartbleed. Sekali lagi Heartbleed bukanlah virus dan heartbleed tidak menyebar atau menginfeksi PC.
3. Jika situs yang digunakan belum kebal terhadap Heartbleed, segera ganti password : Salah. Ganti password setelah situs tersebut dipatch dan kebal terhadap Heartbleed. Mengganti password sebelum situs tersebut kebal terhadap Heartbleed sama artinya dengan memberikan kesempatan kepada sang attacker untuk mencuri detail password baru.

**Cara menghentikan kebocoran dan menanggulangi dampak Bug Heartbleed**

Selama versi rentan OpenSSL masih dipergunakan, ia tetap bisa disalahgunakan. Saat ini, Fixed OpenSSL telah dirilis dan diterapkan. Para penyedia layanan sistem operasi (OS), sistem distribusi dan peralatan multifungsi, pengembang dan penerbit perangkat lunak independen, semua harus mengadopsi perbaikan keamanan tersebut dan menginformasikannya pada klien mereka. Penyedia dan pengguna layanan harus menginstal pemutakhiran ini segera setelah ia tersedia untuk seluruh operating system dan software mereka.

**Apakah CVE-2014-0160 itu?**

CVE-2014-0160 adalah referensi resmi untuk bug ini. CVE (Common Vulnerabilities and Exposures) adalah Standard for Information Security Vulnerability Names yang dikelola oleh MITRE.

**Darimana asal usul nama Heartbleed Bug?**

Bug ini ada dalam implementasi ekstensi heartbeat (RFC6520) TLS/DTLS (transport layer security protocols) OpenSSL. Ketika ekstensi ini dieksploitasi, ia akan mengakibatkan kebocoran konten memori dari server ke client dan dari client ke server.

**Apakah ciri khas Bug Heartbleed?**

Di dalam setiap perangkat lunak atau library selalu ada bug yang umumnya bisa diatasi dengan pemutakhiran versi yang lebih baru. Namun dalam kasus ini, bug yang ada telah mengekspos sejumlah besar private keys dan rahasia (individu maupun lembaga) di internet. Dengan mempertimbangkan cukup lamanya waktu yang telah dilampaui, kemudahan eksploitasi, dan nihilnya jejak penyerangan, bug ini harus ditangani dengan serius.

**Apakah ini sebuah cacat desain pada spesifikasi protokol SSL/TLS?**

Tidak. Ini adalah problem dalam aspek implementasi, yakni kesalahan pemrograman pada library populer OpenSSL yang menyajikan layanan penyandian (crytographic) sejenis SSL/TLS bagi berbagai aplikasi dan service.

**Apa saja yang dibocorkan?**

Enkripsi berfungsi untuk melindungi rahasia-rahasia yang bisa membahayakan privasi atau keamanan Anda apabila bocor. Untuk mengkoordinasi perbaikan atas bug ini, kami telah mengklasifikasikan jenis-jenis rahasia yang bocor ke dalam empat kategori: 1) primary key material, 2) secondary key material, 3) konten yang terproteksi, 4) collateral.

**Apakah kebocoran primary key material itu? Bagaimana penanggulangannya?**

Ini adalah materi utama yang sangat berharga: kunci enkripsi itu sendiri. Secret keys yang bocor mamampukan penyerang untuk mendekripsi lalu lintas – yang sudah lewat maupun yang akan datang – pada layanan yang terproteksi, serta meniru atau menyamar sebagai layanan itu sendiri. Segala bentuk proteksi oleh sistem enkripsi maupun signature pada sertifikat X.509 dapat ditembus.

Penanggulangan atas kebocoran ini membutuhkan:  
– patch pada sisi yang rentan,  
– pembatalan kunci-kunci yang telah terungkap,  
– juga penerbitan dan distribusi ulang keys terkait.

Bahkan semua tindakan tersebut masih menyisakan resiko, yakni pada lalu lintas yang telah disusupi pada waktu yang lampau yang masih rentan terhadap dekripsi. Proses penanggulangan di atas harus dilakukan oleh pemilik layanan sendiri.

**Apakah kebocoran secondary key material itu? Bagaimana mengatasinya?**

Contohnya adalah kredensial pengguna (username dan password) yang digunakan pada situs yang rentan. Untuk mengatasinya, pemilik layanan harus mengembalikan kepercayaan pada layanannya sesuai dengan uraian sebelumnya. Sesudahnya, pengguna akan mengganti password mereka – bisa jadi termasuk kunci enkripsi – sesuai dengan instruksi penyedia layanan. Semua session keysdan session cookies harus diinvalidasi dan dianggap telah tercuri.

**Apakah kebocoran konten terproteksi itu? Bagaimana memperbaikinya?**

Protected content (konten terproteksi) adalah konten aktual yang ditangani oleh layanan yang rentan. Isinya bisa berupa rincian keuangan, komunikasi pribadi seperti email atau pesan instan, dokumen atau apa saja yang dianggap penting untuk diproteksi dengan enkripsi.

Hanya penyedia layanan yang paling mengerti apa saja yang diperkirakan bocor dan wajib memberitahukannya kepada penggunanya. Yang paling penting adalah mengembalikan kepercayaan untuk key material primer dan sekunder seperti uraian sebelumnya. Hanya ini cara untuk mewujudkan penggunaan yang aman atas layanan yang telah terkena bug heartbleed.

**Apakah kebocoran collateral itu? Bagaimana menutupnya?**

Kebocoran collateral adalah keseluruhan rincian lainnya yang telah terekspos kepada penyerang melalui memori konten yang bocor. Isinya bisa berupa rincian teknis seperti alamat memori dan standar keamanan semisal canaries yang yang dipergunakan untuk melindungi dari serangan berkelanjutan. Elemen-elemen ini hanya memiliki nilai-nilai semasa yang akan menjadi tak berharga lagi bagi penyerang sesudah OpenSSL ditingkatkan ke fixed version.

**Apa saja versi OpenSSL yang terkena Heartbleed Bug?**

Status beberapa versi:

* OpenSSL 1.0.1 hingga 1.0.1f (inklusif) – rentan
* OpenSSL 1.0.1g – aman
* OpenSSL 1.0.0 dan cabang-cabangnya – aman
* OpenSSL 0.9.8 dan cabang-cabangnya – aman

Bug ini mulai ada dalam OpenSSL sejak Desember 2011 -> mulai menyebar luas sejak rilis OpenSSL 1.0.1 pada 14 Maret 2012 -> diatasi sejak rilis OpenSSL 1.0.1g pada 7 April 2014.

**Apa saja Sistem Operasi yang terkena bug Heartbleed?**

Ini adalah sejumlah distribusi operating system yang dirilis dengan versi OpenSSL yang rentan:

* Debian Wheezy (stable), OpenSSL 1.0.1e-2+deb7u4
* Ubuntu 12.04.4 LTS, OpenSSL 1.0.1-4ubuntu5.11
* CentOS 6.5, OpenSSL 1.0.1e-15
* Fedora 18, OpenSSL 1.0.1e-4
* OpenBSD 5.3 (OpenSSL 1.0.1c 10 Mei 2012) dan 5.4 (OpenSSL 1.0.1c 10 Mei 2012)
* FreeBSD 10.0 – OpenSSL 1.0.1e 11 Feb 2013
* NetBSD 5.0.2 (OpenSSL 1.0.1e)
* OpenSUSE 12.2 (OpenSSL 1.0.1c)
* Distribusi sistem operasi berikut aman:
* Debian Squeeze (oldstable), OpenSSL 0.9.8o-4squeeze14
* SUSE Linux Enterprise Server
* FreeBSD 8.4 – OpenSSL 0.9.8y 5 Feb 2013
* FreeBSD 9.2 – OpenSSL 0.9.8y 5 Feb 2013
* FreeBSD 10.0p1 – OpenSSL 1.0.1g (At 8 Apr 18:27:46 2014 UTC)
* FreeBSD Ports – OpenSSL 1.0.1g (At 7 Apr 21:46:40 2014 UTC)

**Bagaimana Heartbeat dapat menjadi celah**

Seperti yang sebelumnya disebutkan heartbeat adalah salah satu  fitur OpenSSL yang berfungsi mengecek apakah computer user masih terhungung ke server atau tidak.Heartbeat ini berfungsi seperti saat router yang menjadi perantara antara komputer user dengan server di internet memutuskan hubungan jika terjadi idle yang terlalu lama. Dengan heartbeat, komputer user bisa mengetahui apakah masih terhubung dengan server yang dituju.  
Prinsip kerjanya kurang lebih seperti ini, komputer user akan mengirimkan pesan berisi sebuah magic word dan jumlah karakter kata tersebut. Nanti server akan membalas pesan tersebut dengan menyebutkan magic word tersebut.  
Fasilitas heartbeat tersebut memiliki kelemahan karena terlalu percaya dengan komputer pengirim. komputer attacker cuma mengirimkan sebuah kata yang pendek (seperti melati) namun meminta respon sebanyak 100 karakter. Server ternyata tidak mengecek kalau melati hanya memiliki 6 karakter. Server langsung “memuntahkan” semua karakter yang tersimpan di memori RAM-nya untuk memenuhi permintaan 100 karakter tersebut.  
Dan 100 karakter hanyalah ilustrasi. Sang attacker bisa meminta sampai 64.000 karakter.

Bagi Pengelola Situs

Langkah-langkah penanganan Heartbleed untuk SSL Certificates dari Symantec, RapidSSL, dan Thawte:

Langkah ke 1: Untuk menentukan apakah Anda termasuk yang rentan terkena bug Heartbleed, masukkan nama domain Anda pada https://www.ssllabs.com/ssltest/index.html. Apabila website Anda hasilnya bersih seperti gambar dibawah ini, maka Anda tidak memerlukan tindakan apapun.

Namun, jika website Anda ditemukan rentan terkena bug Heartbleed, Anda harus segera melakukan langkah ke 2 di bawah ini.

Langkah ke 2: Install update versi terbaru dari OpenSSL pada Server Anda. Anda dapat menemukan versi ini disini: https://rhn.redhat.com/errata/RHSA-2014-0376.html. Anda juga dapat mengetahui saran keamanan untuk OpenSSL dari URL berikut: https://www.openssl.org/news/secadv\_20140407.txt.

Langkah ke 3: Buat Certificate Signing Request (CSR) dan Private Key terbaru dari OpenSSL Anda. File CSR yang baru kemudian digunakan untuk menerbitkan ulang Sertifikat SSL Anda (Reissue the certificate) sekaligus Anda gunakan dengan Private Key yang baru untuk diinstall ulang setelah Sertifikat SSL selesai diterbitkan ulang.

Langkah ke 4: Login ke http://www.warungssl.com/logon dan klik di menu "List Orders".

Langkah ke 5: Cari Sertifikat SSL Anda yang akan di-reissue pada daftar tabel dan klik pada No. "Vendor OrderID" pada Sertifikat SSL yang berstatus Active.

Langkah ke 6: Kemudian scroll ke halaman bawah, dan klik pada tombol "Re-issue Certificate".

Langkah ke 7: Kemudian paste hasil CSR baru yang telah dibuat dari versi OpenSSL terbaru, kemudian lengkapi kembali informasi detail yang dibutuhkan, dan klik pada tombol "Submit".

Langkah ke 8: Setelah disubmit, Otoritas Sertifikat Anda akan meminta Anda untuk memverifikasi kepemilikan domain Anda kembali.

Langkah ke 9: Setelah proses verifikasi tentang kepemilikan domain Anda selesai, Sertifikat SSL telah diterbitkan kembali dan Anda dapat melanjutkan untuk menginstall kembali Sertifikat SSL Anda yang telah diterbitkan ulang.

Langkah ke 10: Setelah langkah ke 9 selesai, Anda sudah dapat memenuhi langkah pengamanan dengan baik. Namun, harap dicatat bahwa sertifikat SSL anda yang lama secara otomatis akan dicabut oleh Otoritas Sertifikat dalam waktu 12 jam setelah Anda melakukan reissue Sertifikat SSL. Namun, apabila Anda tidak ingin menunggu 12 jam, Anda dapat menghubungi langsung Otoritas Sertifikat dengan menginformasikan bahwa Sertifikat SSL yang baru setelah direissue telah diinstall pada Server Anda, dan meminta Otoritas Sertifikat untuk mencabut Sertifikat SSL yang lama secara manual (SSL Revocation).  
  
Langkah penanganan Heartbleed untuk SSL Certificates dari GeoTrust dan Comodo:

Langkah ke 1: Untuk menentukan apakah Anda termasuk yang rentan terkena bug Heartbleed, masukkan nama domain Anda pada https://www.ssllabs.com/ssltest/index.html. Apabila website Anda hasilnya bersih seperti gambar dibawah ini, maka Anda tidak memerlukan tindakan apapun. Namun, jika website Anda ditemukan rentan terkena bug Heartbleed, Anda harus segera melakukan langkah ke 2 dibawah ini.

Langkah ke 2: Install update versi terbaru dari OpenSSL pada Server Anda. Anda dapat menemukan versi ini disini: https://rhn.redhat.com/errata/RHSA-2014-0376.html. Anda juga dapat mengetahui saran keamanan untuk OpenSSL dari URL berikut: https://www.openssl.org/news/secadv\_20140407.txt.

Langkah ke 3: Buat Certificate Signing Request (CSR) dan Private Key terbaru dari OpenSSL Anda. File CSR yang baru kemudian digunakan untuk menerbitkan ulang Sertifikat SSL Anda (Reissue the certificate) sekaligus Anda gunakan dengan Private Key yang baru untuk diinstall ulang setelah Sertifikat SSL selesai diterbitkan ulang.

Langkah ke 4: Periksa nomor seri Sertifikat Anda dan simpan kedalam file notepad pada Desktop Anda. Anda akan membutuhkan informasi ini secara manual pada saat mencabut Sertifikat SSL lama Anda yang berdapampak rawan keamanan Heartbleed. Anda dapat mengetahui informasi nomor serial ini dengan mengklik pada ikon gembok disamping URL Anda pada saat mengakses melalui browser. Silahkan melihat seperti gambar di bawah ini:

Langkah ke 5: Login ke http://www.warungssl.com/logon dan klik di menu "List Orders".

Langkah ke 6: Cari Sertifikat SSL Anda yang akan di-reissue pada daftar tabel dan klik pada No. "Vendor OrderID" pada Sertifikat SSL yang berstatus Active.

Langkah ke 7: Kemudian scroll ke halaman bawah, dan klik pada tombol "Re-issue Certificate".

Langkah ke 8: Kemudian paste hasil CSR baru yang telah dibuat dari versi OpenSSL terbaru, kemudian lengkapi kembali informasi detail yang dibutuhkan, dan klik pada tombol "Submit".

Langkah ke 9: Setelah disubmit, Otoritas Sertifikat Anda akan meminta Anda untuk memverifikasi kepemilikan domain Anda kembali.

Langkah ke 10: Setelah proses verifikasi tentang kepemilikan domain Anda selesai, Sertifikat SSL yang telah diterbitkan ulang dapat Anda lanjutkan untuk diinstall kembali pada server Anda.

Langkah ke 11: Setelah proses instalasi SSL Anda selesai, selanjutnya lakukan proses pencabutan Sertifikat SSL (Revoke SSL) yang lama secara manual dengan cara melakukan klik pada tombol Revocation di bawah ini.

Langkah ke 12: Setelah tombol Revocation diklik, Anda akan dialihkan ke websitehttps://www.centralapi.com/heartbleed.aspx, dimana kami akan menanyakan informasi username dan password Anda, beserta dengan Nomor pemesanan (Order Number) Anda serta Nomor Seri dari Sertifikat SSL yang telah Anda dapatkan seperti langkah No. 4 untuk mencabut Sertifikat SSL yang lama.

**Seberapa serius situasi ini**

Secara teori, OpenSSL bekerja dengan baik. Namun terdapat kesalahan kecil pada kode sumber seperti Heartbleed. Dan Akibatnya telah membuat pustaka perangkat lunak dan versi populer berakit lemah keamanan. Hampir semua versi pada OpenSSL yang terkena mampu memberikan akses pribadi pada website yang seharusnya menjadi aman karena kode TLS/SSL.

Dalam situasi ini, para penyerang secara teori bisa melihat isi dari kode rahasia (secret handshake) pada saat sesi SSL terjalin ketika pengguna melakukan login ke account mereka seperti saat login pada email account. Username dan password, bahkan hingga informasi nomor Kartu Kredit sangat mungkin beresiko, dan tergantung pada layanan apa yang sedang diakses oleh pengguna meskipun belum ada cara untuk mengetahui hal ini dengan pasti. Penyerang dapat mengidentifikasi dirinya di Internet. Setelah setengah proses jabat tangan (SSL handshake) terganggu melalui cara ini, penyerang dapat menggunakan private key baru mereka untuk melakukan serangan yang disebut dengan serangan "Man-in-the-middle".

**Apa yang bisa didapatkan dengan Heartbleed ini?**  
Semuanya yang bisa disimpan dalam memori komputer akan bisa didapatkan, tinggal seberapa betahnya si penyerang meretas mengumpulkan informasi. Masalahnya yang diserang tidak akan mengetahui adanya tindakan ini karena tidak ada cara mendeteksinya secara langsung, yang bisa dilakukan oleh pemilik website adalah menganalisa log (catatan) akses pengunjung. Jadi username, email, password, nomor kartu kredit, private key dan yang lainnya ada kemungkinan bisa didapatkan.  
  
**Berikut deskripsi cara kerja Heartbleed:**  
  
Belakangan ini Heartbleed ramai disebut sebagai salah satu celah keamanan terbesar dan tercanggih yang pernah ditemukan sepanjang sejarah internet. Heartbleed ditemukan setelah tim peneliti keamanan komputer di Universitas Michigan, Amerika Serikat, menggunakan pemindai jaringan open source yang disebut ZMap. ZMap dikembangkan di Universitas Michigan oleh Asisten Profesor J Alex Halderman dan mahasiswa pascasarjana ilmu komputer, Zakir Durumeric dan Eric Wusterow. Zmap berguna untuk mencari server internet yang rentan terhadap Heartbleed yang berpotensi digunakan untuk mencuri username, password, dan informasi penting lain.  
  
Celah keamanan ini ditemukan pada OpenSSL, sebuah protokol sekuriti open-source yang digunakan untuk enkripsi informasi sensitif melalui fungsi SSL (secure sockets layer) di banyak layanan berbasis internet.  
  
Heartbleed berimbas pada semua situs web dan layanan yang menjalankan OpenSSL versi 1.0.1 hingga 1.01f. Versi-versi OpenSSL yang rawan tersebut sudah banyak dipakai sejak Mei 2012.  
Artinya, selama dua tahun, bug ini telah beredar tanpa terdeteksi di semua penyedia layanan yang menggunakan enkripsi OpenSSL, mulai dari aplikasi, situs web internet, hingga institusi perbankan.  
  
Masalahnya menjadi besar karena OpenSSL digunakan oleh 66 persen dari semua bagian web internet untuk mengenkripsi data sehingga celah keamanan tersebar luas.  
  
Sebagian nama layanan yang terkena dampak Heartbleed bisa dilihat dalam sebuah daftar yang dibuat pada 8 April 2014. Semenjak daftar tersebut dipublikasikan, beberapa penyedia layanan, seperti Facebook, Yahoo, Gmail, Tumblr, dan Dropbox, telah menyalurkan patch untuk menambal celah keamanan yang ada.

http://www.kaskus.co.id/thread/5351212a0d8b46f53f8b478c

Bagaimana Cara Melindungi dan Mencegah Heartbleed ?

Bug Heartbleed ini ditemukan pertama kali oleh Google Security team dan software yang bernama Codenomicon. kita patut berterimakasih kepada mereka karena berkat mereka hingga saat ini dari data yang diterima dinyatakan bahwa tidak/beluma ada satu aksi pun yang di ambil oleh para Hacker maupun cracker tersebut karena celah ini ditemukan oleh security team tersebut pertama kali. namun, apa salahnya jika kita mengetahui bagaimana cara melindungi dan mencegah dari bug heartbleed ini.

1. Langkah Pertama, silahkan cek apakah situs yang biasa anda gunakan terinfeksi oleh bug ini atau tidak. jika anda mau mengecek daftar panjang website yang terkena dampaknya , anda bisa bisa mengecek situs tersebut dengan Heartbleed Checker yang di buat oleh password security LastPass. disitu anda bisa memasukan alamat website yang ingin anda cek.

2. Selanjutnya, ganti password akun , email, banking pada website yang terinfeksi oleh heartbleed namun website tersebut harus sudah melakukan patch terhadap heartbleed. Jika website tersebut belum melakukan patch, tentunya akan sulit karena percuma kita mengganti password kecuali kita menanyakan kepada pihak website tersebut untuk segera melakukan patch terhadap sistem keamanan mereka.

3. Yang penting diperhatikan adalah website yang memiliki informasi penting diri kita seperti Yahoo, facebook dan Gmail. dimana pengguna diharuskan melakukan pergantian password mereka jika mereka memiliki data yang dirasa penting dan sangat rahasia.

Daftar Website yang terkena dampak Heartbleed

Berikut ini merupakan daftar nama - nama website yang terkena dampak Heartbleed, anda bisa melakukan pencarian dengan menggunakan shortcut CTRL + F untuk mempermudah pencarian. daftar ini admin sadur dari website Mashable.

TABEL BELUM DICOPY

http://blog.sslmurah.com/tutorial/istilah/definisi-heartbleed-bug-apa-itu/#more-1301

De\_nisi Heartbleed Bug, Apa itu?

Akhir-akhir ini sedang heboh di dunia Internet akan adanya Heartbleed, ini kalau diartikan secara har\_ah

sangar dan menyeramkan, yaitu jantung yang berdarah-darah. Heartbleed sendiri artinya adalah Sebuah

kerentanan kritis yang dijuluki “Heartbleed” ditemukan di OpenSSL, modul SSL yang paling populer

digunakan pada server Linux / cPanel. Ini memungkinkan pihak ketiga mengeksploitasi untuk mencuri

informasi yang seharusnya dapat dijamin dan dienkripsi dengan protokol SSL / TLS, dan mencuri kunci

pribadi dari pasangan serti\_kat itu sendiri.

Heartbleed Bug adalah kerentanan serius dalam perpustakaan kriptogra\_ perangkat lunak populer

OpenSSL. Kelemahan ini memungkinkan orang lain mencuri informasi yang dilindungi, dalam kondisi normal

maupun enkripsi SSL / TLS yang digunakan untuk mengamankan Situs di Internet. SSL / TLS memberikan

keamanan dan privasi komunikasi melalui Internet untuk aplikasi seperti web, email, instant messaging (IM)

dan beberapa jaringan pribadi virtual (VPN).

Heartbleed bug memungkinkan setiap orang di Internet untuk membaca memori sistem yang dilindungi

oleh perangkat lunak OpenSSL versi rentan. Ini kompromi kunci rahasia yang digunakan untuk

mengidenti\_kasi penyedia layanan dan untuk mengenkripsi lalu lintas, nama dan password pengguna dan

konten yang sebenarnya. Hal ini memungkinkan penyerang untuk menyadap komunikasi, mencuri data

langsung dari layanan dan user dan untuk meniru layanan dan user.

Jenis Kerentanan

Para pakar internet telah menguji beberapa

layanan mereka sendiri dari perspektif penyerang.

Mereka menyerang diri mereka sendiri dari luar,

tanpa meninggalkan jejak. Tanpa menggunakan

informasi rahasia atau kredensial mereka mampu

mencuri dari diri mereka sendiri kunci rahasia

yang digunakan untuk serti\_kat X.509 mereka,

nama pengguna dan password, pesan instan,

email dan dokumen bisnis penting dan

komunikasi.

Bagaimana menghentikan kerentanan ini?

Selama versi rentan OpenSSL sedang digunakan dalam sebuah website maka dapat disalahgunakan.

OpenSSL telah dirilis dan sekarang itu harus dikerahkan. Vendor sistem operasi dan distribusi, vendor alat,

vendor software independen harus mengadopsi memperbaiki dan memberitahu pengguna mereka.

Penyedia layanan dan pengguna harus menginstal perbaikan seperti yang tersedia untuk sistem operasi,

peralatan jaringan dan perangkat lunak yang mereka gunakan.

Anda dapat melakukan perubahan password secara berkala, apakah itu sebulan sekali, untuk mengurangi

kemungkinan buruk yang terjadi, sebab memang standar pengelolaan akun adalah dengan mengubah

password secara berkala.

OpenSSL telah berusaha sekuat tenaga untuk mengatasi hal ini dan memberikan versi baru bagi setiap

website. Anda yang telah menggunakan Serti\_kat dari Kami ada baiknya untuk melakukan re-issue pada

dashboard Anda. Sebelum melakukannya, harap untuk memback up semua data apa saja, baik dari yang

kecil hingga yang besar dari server website Anda. Dengan menginstal versi baru maka situs Anda

kemungkinan Aman dari serangan.

Heartbleed dapat menyerang situs ber-SSL maka akan sangat mudah pula untuk menyerang situs tanpa

Serti\_kat SSL, untuk itu pasanglah segera untuk melakukan pengamanan tingkat lanjut.

https://mansyth.wordpress.com/tag/pengertian-heartbleed/

Heart Bleed

Beberapa bulan yang lalu saat gw lagi asik browsingan gw dikejutkan sama sesuatu yang berbahaya,

dan itu dinamakan dengan ” Heart Bleed”, dari namanya aja kedengaranya udah ngeri banget coy,

kalo kata heartnya sih oke lah, so sweet gitu..eh tapi kata bleednya itu loh, berdarah darah. nah loh?

Gw kira ini tuh semacam penyakit baru hasil kontrasepsi..eh heh maksud gw konspirasi mamarika

yang lagi menyebar dan menjangkit para penduduk diseluruh dunia termasuk indonesia, lah terus gw

panik donk, setelah penyakit cikungunya yang pernah gw rasain bener-bener nggak enak coy,

apalagi nih penyakit yang pake ada berdarah-darah segala. karena gw penasaran akhirnya gw coba

cari aja tuh tentang tuh penyakit, hahahahhaa. Setelah baca artikel demi artikel gw pun bisa berlega

ria coy, ternyata itu bukan penyakit yang menyerang manusia, tapi penyakit yang menyerang

sebuah protokol keamanan di internet, jadi intinya dia itu ( heartbleed) adalah bug yang

memanfaatkan kelemahan yang ada pada protokol keamanan (SSL) lalu dengan cepatnya

mengambil data pribadi para pengguna internet yang tersimpan diserver. Yang pasti ini sesuatu yang

bikin setiap orang panik dan sangat berbahaya bagi mereka yang sering mencantumkan password

mereka diinternet dari password jejaring sosial sampe akun perbankan, kalo mau lebih detailnya cek

dibawah coy.

APA ITU SSL ?

SSL adalah kependekan dari Secure Socket Layer yang merupakan suatu protocol layer transport

yang digunakan dalam koneksi internet secara aman. Jika anda menginginkan suatu koneksi

komunikasi lewat internet dengan cara yang secure, maka gunakan koneksi SSL.

SSL menawarkan tiga tingkat keamanan, yaitu:

Authentication: Memastikan bahwa message yang diterima berasal dari seseorang yang tersurat

Confidentiality: Melindungi pesan dari suatu usaha pembacaan oleh penerima yang tidak

berhak disepanjang perjalanannya.

Integrity: Memastikan bahwa pesan asli, tidak mengalami perubahan dalam perjalanannya.

SSL dikembangkan oleh Netscape Communications agar bisa mengirim data secara aman lewat

internet. Jika anda pernah memperhatikan di browser internet dengan menggunakan HTTPS, maka

koneksi internet ini adalah menggunakan SSL yang umum digunakan pada suatu transaksi online.

Jadi HTTPS adalah suatu protocol untuk melakukan transfer data yang terinkripsi melalui web.

PERBEDAAN HTTP DAN HTTPS

HTTPS melakukan koneksi melalui port 443, sementara HTTP menggunakan port 80

HTTPS mengirim / menerima data dengan inkripsi lewat protocol SSL, sementara HTTP mengirim

data dengan plain text

Jadi dalam transaksi online, maka pastikan anda melihat online store anda menggunakan HTTPS

dalam bertransaksi keuangan lewat internet.

Jika anda mempunyai website, apa yang diperlukan agar bisa di host disuatu host yang bisa SSL.

Web server haruslah support inkripsi SSL

IP address public yang unik agar penyedia certificate SSL bisa melakukan validasi website anda

Suatu certificate SSL dari penyedia layanan SSL

Dua yang pertama bisa anda dapatkan dari ISP anda, hubungi ISP anda untuk memastikannya.

SSL beroperasi pada antara layer Application dan Transport pada model OSI (http://www.jaringankomputer.

cv-sysneta.com/model-referensi-osi). SSL tidak bekerja secara transparent automatis, karena

hanya bisa kalau memang protocol-protocol applikasi secara explicit memang diimplementasikan.

SSL menggunakan inkripsi public-key untuk maksud authentication dan inkripsi symmetric key

untuk inkripsi informasi yang dikirim. Untuk public key inkripsi SSL menggunakan algoritma

inkripsi Rivest-Shamir-Adleman (RSA), makanya bergantung pada implementasi dari infrastructure

public key (PKI) yang didukung. Integritas pesan dijamin dengan cara mekanisme checking integritas

yang disebut sebagai message authentication code (MAC).

Proses authentikasi

Suatu sesi SSL bermula saat suatu client dengan SSL-enabled meminta suatu koneksi dengan server

Suatu sesi SSL bermula saat suatu client dengan SSL-enabled meminta suatu koneksi dengan server

dengan SSL-enabled melalui TCP port 443, yaitu port SSL. Hal ini akan menginisiasi suatu koneksi

SSL antara client dan server. Semua website yang menggunakan SSL mempunyai suatu URL dengan

awalan HTTPS. Server kemudian mengirimkan certificate digital dan public key kepada client

tersebut.

Client server kemudian melakukan negosiasi tingkat inkripsi mana yang bisa diterima yang biasanya

40-bit, 56-bit, ataupun 128 bit keatas. Client kemudian menghasilkan suatu secret session key yang

kemudian di inkripsi menggunakan public key dari server untuk kemudian mengirimkan nya kepada

server. Server kemudian melakukan dekripsi secret session key tersebut menggunakan private keynya.

Dari poin ini seterusnya, secret key cryptography dikenakan dan kemudian session key

digunakan untuk meng-inkripsi semua pertukaran data antara client dan server, memberikan suatu

komunikasi private yang aman.

SSL ini tentunya tidak bebas dari masalah begitu saja. Semua transaksi web dengan SSL akan

menambah overhead pemrosesan pada server. Terkadang menjadi dua kali lipat tingkat overhead

prosessingnya dibanding tanpa menggunakan koneksi secure SSL. Dengan hardware mesin yang

sama, maka tingkat beban prosessing dengan menggunakan SSL akan menjadi sangat berat

dibanding tanpa SSL.

Disamping itu, SSL jadi sulit diimplementasikan dalam e-commerse yang menggunakan web server

farms dan server load balancers (http://www.jaringan-komputer.cv-sysneta.com/solusi-cluster-server).

Hal ini mengingat SSL didesign agar client menggunakan IP address yang sama selama sessi

berlangsung.

Untuk mengatasi masalah ini, biasanya digunakan hardware khusus yang disebut SSL Accelerators

untuk mengambil alih beban processing dan sesi cache kepada server-server lain untuk meningkatkan

performa.

APA ITU HEARTBLEED ?

Heartbleed adalah bug yang memanfaatkan kelemahan di OpenSSL. Dinamakan Heartbleed karena

bug ini memanfaatkan fasilitas heartbeat yang ada di OpenSSL

APA ITU HEARTBEAT?

Heartbeat itu salah satu fitur OpenSSL yang diperkenalkan tahun 2012. Tujuan heartbeat adalah

mengecek apakah komputer kamu masih terhubung ke sebuah server. Soalnya, seringkali router—

yang menjadi perantara antara komputer kamu dengan server di internet—memutuskan hubungan

jika terjadi idle yang terlalu lama. Dengan heartbeat, komputer kamu bisa mengetahui apakah masih

terhubung dengan server yang dituju.

Prinsip kerjanya kurang lebih seperti gambar di bawah: komputer kamu akan mengirimkan pesan

berisi sebuah magic word dan jumlah karakter kata tersebut. Nanti server akan membalas pesan

tersebut dengan menyebutkan magic word tersebut.

CARA MEMANFAATKAN HEARTBEAT?

Fasilitas heartbeat ini memiliki kelemahan karena terlalu percaya dengan komputer pengirim.

Misalnya seperti contoh dibawah adalah interaksi antar komputer pribadi dengan server,

pc : hey server, kita berdua masih nyambung nggak koneksinya?

server : masih kok bro, emang ada apa?

pc : gw pengen login nih, tapi nggak bisa, kata kuncinya tuh donidoni, panjang karakternya 100

karakter.

server : oke, data lo nih ” donidoni#%#satu : 09/05/1994 : doni.antara@gmail.com : password

sayakeren.

komputer hacker cuma mengirimkan sebuah kata yang pendek (seperti donidoni) namun meminta

respon sebanyak 100 karakter. Server ternyata tidak mengecek kalau donidoni hanya memiliki

beberapa karakter. Server langsung “memuntahkan” semua karakter yang tersimpan di memori

RAM-nya untuk memenuhi permintaan 100 karakter tersebut.

Dan 100 karakter hanyalah ilustrasi. Sang hacker bisa meminta sampai 64.000 karakter.

DATA YANG DISIMPAN DI MEMORY SERVER?

Banyak sekali, termasuk informasi sangat rahasia. Atas nama kecepatan, server secara terus-menerus

akan menyimpan berbagai data di memorinya. Seperti contoh di atas, memori server bisa menyimpan

data nama, alamat email, tanggal lahir, password, sampai nomor kredit kamu. Yang lebih berbahaya,

private key pun bisa disimpan di memori. Fyi, private key adalah kunci rahasia yang digunakan

server untuk membuka teks yang diacak oleh OpenSSL tersebut. Private key ini seharusnya hanya

diketahui oleh sistem. Jika diketahui hacker, berarti semua data yang diacak tersebut bisa dibuka sang

hacker dengan mudah.

TERUS KITA HARUS GIMANA NIH ?

Bug Heartbleeding ini sebenarnya tanggung jawab penyedia situs. Mereka harus mengganti

OpenSSL ke versi terbaru, sekaligus membuat private key baru. Untungnya, sang penemu

Heartbleed telah menginformasikan bug ini ke OpenSSL Foundation sebelum mengumumkannya ke

publik. Alhasil, banyak situs yang telah menanggulangi bug ini sebelum berita resminya beredar,

seperti Facebook, Google, dan beberapa situs besar lain.

Namun karena OpenSSL digunakan di sepertiga situs di internet (atau sekitar 500 juta situs), masih

banyak yang harus diperbaiki. Dan yang membuat Heartbleed berbahaya adalah tidak ada jejak

sedikitpun yang menunjukkan apakah situs tersebut pernah dijebol menggunakan Heartbleed.

CEK APAKAH SITUS TERJANGKIT ATAU TIDAK ?

Coba cek di situs LastPass (https://lastpass.com/heartbleed/) ini. LastPass akan melihat engine di balik

situs tersebut. Jika menggunakan Apache atau Nginx, dua database engine yang menggunakan

OpenSSL, situs tersebut dinyatakan rentan (meskipun belum tentu sudah dibobol). Kamu juga bisa

melihat ke artikel Mashable (http://mashable.com/2014/04/09/heartbleed-bug-websites-affected/) ini

yang mendaftar situs populer yang telah atau belum menambal kelemahan Heartbleed ini.

CARA AGAR DATA TIDAK DICURI ?

Cara paling aman adalah tidak login ke situs tersebut untuk sementara waktu—sebelum mereka

mengganti OpenSSL-nya ke generasi terbaru. Jika mereka sudah melakukan itu, baru kamu ganti

password-nya dengan yang baru.

Dan ingat-ingat username dan password lama yang kamu gunakan di situs tersebut. Jika password itu

kita gunakan di situs lain (situs B, misalnya), ganti password di situs B. Takutnya, sang hacker berhasil

mendapatkan password kamu di situs A lalu menggunakannya di situs B.

YANG BIKIN BUG HEARTBLEED ?

Eksperimen heartbeat ditambahkan oleh Robin Seggelmen, seorang programmer asal Jerman, pada

tahun 2011, dan dirilis ke publik pada tahun 2012. Namun ia menyangkal kelemahan itu dilakukan

secara sengaja. Kode itu pun lolos dari validasi yang dilakukan Dr Stephen Henson yang merupakan

salah satu anggota inti OpenSSL Foundation.

HEARTBLEED KETAUAN SAMA SIAPA SIH?

Dia adalah Neel Mehta, salah satu anggota Google Security. Atas jasanya tersebut, dia mendapatkan

uang sebesar US$ 15 ribu dari Internet Bug Bounty. Namun oleh Neel, uang itu langsung

disumbangkan kepada yayasan The Freedom of Press Foundation yang bergerak di bidang

keamanan komunikasi digital.

SUMUR :

http://www.jaringan-komputer.cv-sysneta.com/apa-itu-secure-socket-layer-ssl (http://www.jaringankomputer.

cv-sysneta.com/apa-itu-secure-socket-layer-ssl)

http://www.pcplus.co.id/2014/04/fitur/apa-itu-heartbleed/ (http://www.pcplus.co.id/2014/04/fitur/apaitu-

heartbleed/)

http://kaharsan.blogspot.com/2014/04/pengertian-dan-cara-mengatasi.html

Belakangan ini apa agan pernah mendengar tentang isu di Internet tentang Heartbleed ? bagaimana media

luar seperti Mashable dan media lokal seperti Kompas, detik dan yang lainnya menyebutkan bahwa kita

diwajibkan untuk mengganti password sejumlah akun website dan social media seperti facebook dan gmail

?

nah isu ini sebenarnya sudah lama sekali beredar sejak tahun 2011 silam, namun nampaknya pada tahun

itu banyak pihak yang tidak merespon akan adanya heartbleed ini.Apasih Heartbleed itu ?, Bagaimana Cara

mencegah serangan heartbleed ? dan Situs apa saja yang terkena dampak heartbleed. silahkan disimak

dengan baik.

Sebuah kegagalan enkripsi bernama Heartbleed telah berhasil memanggil salah satu celah keamanan

terbesar di Internet yang pernah kita temui. hal ini menular terhadap beberapa situs besar dan

pelayanannya dimana mungkin setiap hari kita memakainya, seperti Gmail, dan Facebook dan mungkin

akibat hal ini, data pribadi kita seperti password dan nomor credit card dapat terlihat oleh pihak - pihak

tertentu.

Nah gara - gara heartbleed ini juga perusahaan rahasia besar yang menggunakan Open SSL juga

kemungkinan besar akan dapat diretas oleh kracker yang menggunakan "kunci Digital" untuk dapat masuk

ke sistem mereka. wah kalau seperti ini tentunya akan menjadi suatu masalah yang sangat serius sekali

dimana orang yang tidak bertanggung jawab dapat dengan mudah memanfaatkan dan menyalahgunakan data kita untuk keperluan mereka.

Bagaimana Cara Melindungi dan Mencegah Heartbleed ?

Langkah Pertama, silahkan cek apakah situs yang biasa anda gunakan terinfeksi oleh bug ini atau tidak. jika

anda mau mengecek daftar panjang website yang terkena dampaknya , anda bisa bisa mengecek situs

tersebut dengan Heartbleed Checker yang di buat oleh password security LastPass. disitu anda bisa

memasukan alamat website yang ingin anda cek

Selanjutnya, ganti password akun , email, banking pada website yang terinfeksi oleh heartbleed

namun website tersebut harus sudah melakukan patch terhadap heartbleed. jika website tersebut

belum melakukan patch, tentunya akan sulit karena percuma kita mengganti password kecuali kita

menanyakan kepada pihak website tersebut untuk segera melakukan patch terhadap sistem

keamanan mereka.

Yang penting diperhatikan adalah website yang memiliki informasi penting diri kita seperti Yahoo,

facebook dan Gmail. dimana pengguna diharuskan melakukan pergantian password mereka jika

mereka memiliki data yang dirasa penting dan sangat rahasia.

Apakah Agan Tau Bahwa Android Bisa Saja Terinfeksi?

BERITA

Sekira 50 juta perangkat berbasis sistem operasi Android rentan terhadap celah keamanan Heartbleed Bug.

Menurut data yang dilaporkan The Guardian, angka ini lebih mengkhawatirkan ketimbang perkiraan sebelumnya.

Dilansir Digitaltrends, Kamis (17/4/2014), pengguna Android mungkin lebih rentan terhadap Heartbleed Bug

daripada yang diperkirakan sebelumnya. Sekira 50 juta smartphone dengan OS robot hijau ini, rentan terhadap

bug OpenSSL.

Data ini didasarkan pada pengumuman Google yang dipublikasikan pada 9 April 2014. "Semua versi Android kebal

terhadap CVE-2014-0160, dengan pengecualian terbatas dari Android 4.1.1," tulis Google.

CVE-2014-0160 ini mengacu pada Heartbleed Bug. Menurut perusahaan analisis Chitika, jumlah smartphone di

seluruh dunia yang berjalan di Android 4.1.1 Jelly Bean diperkirakan sekira 50 juta dan 4 juta di antaranya berada

di Amerika Serikat.

Chitika mengungkapkan, selama periode 7-13 April, pengguna Android Jelly Bean (4.1.1) menghasilkan 19 persen

dari total lalu lintas Android 4.1 di Amerika Utara. Sementara versi 4.1.2 menghasilkan 81 persen.

Ada kemungkinan lebih banyak ponsel yang rentan terkena imbas dari Heartbleed Bug. Google belum memberikan

angka konkret terkait berapa banyak smartphone Android yang terkena celah keamanan tersebut.

Namun, perwakilan Google mengestimasi bahwa penggunaan Android 4.1.1 berada di persentase satu digit. Ini

menandakan bahwa sekira 20 sampai 100 juta perangkat Android bisa terpengaruh.

Ponsel Android yang menjalankan Jelly Bean ini dapat diretas menggunakan metode yang disebut 'reverse

Heartbleed'. Ini menunjukkan bahwa server jahat bisa menggunakan kerentanan OpenSSL untuk mengambil data

dari browser pada ponsel pengguna

Sumber

Google sudah mengkonfirmasi bahwa Android 4.1.1 masih vulnerable terhadap Heartbleed. Artinya pengguna

Android 4.1.1 yang jumlahnya ada jutaan orang masih berpotensi menjadi korban dari bug Heartbleed ini. Hacker

masih punya kesempatan untuk mengambil berbagai data penting dan sensitif milik pengguna.

Saat ini Google sudah mengirimkan informasi patch tersebut kepada manufaktur. Sayangnya belum ada kejelasan

kapan Android 4.1.1 akan terupdate dan menjadi kebal terhadap Heartbleed. Bagi kamu pengguna Android 4.1.1,

maka kamu memiliki dua pilihan: melakukan update Android ke versi selain 4.1.1, atau menunggu patch Android 4.1.1 dirilis.

Lookout telah merilis versi terbarunya di Google Play Store dimana memudahkan pengguna untuk

mengecek dan memastikan bahwa Android mereka terkena Heartbleed atau tidak. Aplikasi bernama

Heartbleed Detector, akan mengecek versi dari OpenSSL yang berjalan di Android kamu, dan berdasarkan

informasi tersebut kamu akan mengetahui apakah Android kamu terinfeksi atau tidak. Heartbleed Detector

milik Lookout ini, tidak akan membersihkan atau memperbaiki masalah, karena fungsinya hanya sebagai

pendeteksi apakah kamu terinfeksi oleh bug ini.

Kesimpulannya Heartbleed Detector akan membantu kamu menemukan apa saja yang telah diambil oleh

Heartbleed di Android kamu. Jika Android kamu belum mendapat update patch, segera lakukan

pengecekan agar kamu terhindar dari Heartbleed ini. Jadi untuk itu segera download Lookout Heartbleed

Detector dan install di Android kamu

Download Heartbleed detector VIA PlayStore

Download antivirus lookout VIA PlayStore

Download CM Security Heartbleed Via PlayStore

http://www.pcplus.co.id/2014/04/fitur/apa-itu-heartbleed/

1. Apa itu Heartbleed?

Heartbleed adalah bug yang memanfaatkan kelemahan di OpenSSL. Dinamakan Heartbleed karena bug ini memanfaatkan

fasilitas heartbeat yang ada di OpenSSL

2. Hmm, bisa jelasin istilah-istilah itu gak? Gak terlalu ngerti..

Emang agak teknis sih. Penjelasan gampangnya: SSL itu adalah standar keamanan yang akan mengenkripsi teks (seperti

username dan password) yang kamu kirim via browser. Contohnya ketika kamu buka www.facebook.com dan

memasukkan username dan password kamu, semua teks itu akan diacak dulu. Jadi jika ada hacker yang mencoba

menyabot koneksi dari komputer kamu ke server Facebook cuma akan mendapatkan teks yang diacak dan sulit dibaca.

Nah OpenSSL adalah salah satu teknik SSL tersebut. Dinamakan “open” karena memang bersifat open source. Siapa saja

bisa menyumbang fitur tambahan di OpenSSL ini. Dan karena open source, OpenSSL banyak digunakan di web server yang

membutuhkan proses login.

3. Kalau heartbeat, apaan tuh?

Heartbeat itu salah satu fitur OpenSSL yang diperkenalkan tahun 2012. Tujuan heartbeat adalah mengecek apakah

komputer kamu masih terhubung ke sebuah server. Soalnya, seringkali router—yang menjadi perantara antara komputer

kamu dengan server di internet—memutuskan hubungan jika terjadi idle yang terlalu lama. Dengan heartbeat, komputer

kamu bisa mengetahui apakah masih terhubung dengan server yang dituju.

Prinsip kerjanya kurang lebih seperti gambar di bawah: komputer kamu akan mengirimkan pesan berisi sebuah magic

word dan jumlah karakter kata tersebut. Nanti server akan membalas pesan tersebut dengan menyebutkan magic word

tersebut. 4. Kayaknya gak berbahaya. Kok bisa dimanfaatkan ya?

Fasilitas heartbeat ini memiliki kelemahan karena terlalu percaya dengan komputer pengirim. Seperti ilustrasi di bawah,

komputer hacker cuma mengirimkan sebuah kata yang pendek (seperti melati) namun meminta respon sebanyak 100

karakter. Server ternyata tidak mengecek kalau melati hanya memiliki 6 karakter. Server langsung “memuntahkan” semua

karakter yang tersimpan di memori RAM-nya untuk memenuhi permintaan 100 karakter tersebut.

Dan 100 karakter hanyalah ilustrasi. Sang hacker bisa meminta sampai 64.000 karakter. 5. Emang apa yang disimpan di memori server?

Banyak sekali, termasuk informasi sangat rahasia. Atas nama kecepatan, server secara terus-menerus akan menyimpan

berbagai data di memorinya. Seperti contoh di atas, memori server bisa menyimpan data nama, alamat email, tanggal lahir,

password, sampai nomor kredit kamu. Yang lebih berbahaya, private key pun bisa disimpan di memori. Fyi, private key

adalah kunci rahasia yang digunakan server untuk membuka teks yang diacak oleh OpenSSL tersebut. Private key ini

seharusnya hanya diketahui oleh sistem. Jika diketahui hacker, berarti semua data yang diacak tersebut bisa dibuka sang

hacker dengan mudah.

6. Waduh, terus kita harus gimana nih?

Bug Heartbleeding ini sebenarnya tanggung jawab penyedia situs. Mereka harus mengganti OpenSSL ke versi terbaru,

sekaligus membuat private key baru. Untungnya, sang penemu Heartbleed telah menginformasikan bug ini ke OpenSSL

Foundation sebelum mengumumkannya ke publik. Alhasil, banyak situs yang telah menanggulangi bug ini sebelum berita

resminya beredar, seperti Facebook, Google, dan beberapa situs besar lain.

Namun karena OpenSSL digunakan di sepertiga situs di internet (atau sekitar 500 juta situs), masih banyak yang harus

diperbaiki. Dan yang membuat Heartbleed berbahaya adalah tidak ada jejak sedikitpun yang menunjukkan apakah situs

tersebut pernah dijebol menggunakan Heartbleed.

7. Waduh, situs favorit saya termasuk gak ya?

Coba cek di situs LastPass ini. LastPass akan melihat engine di balik situs tersebut. Jika menggunakan Apache atau Nginx,

dua database engine yang menggunakan OpenSSL, situs tersebut dinyatakan rentan (meskipun belum tentu sudah

dibobol). Kamu juga bisa melihat ke artikel Mashable ini yang mendaftar situs populer yang telah atau belum menambal

kelemahan Heartbleed ini.

8. Kalau benar rentan, kita harus gimana?

Cara paling aman adalah tidak login ke situs tersebut untuk sementara waktu—sebelum mereka mengganti OpenSSL-nya

ke generasi terbaru. Jika mereka sudah melakukan itu, baru kamu ganti password-nya dengan yang baru.

Dan ingat-ingat username dan password lama yang kamu gunakan di situs tersebut. Jika password itu kita gunakan di situs

lain (situs B, misalnya), ganti password di situs B. Takutnya, sang hacker berhasil mendapatkan password kamu di situs A

lalu menggunakannya di situs B.

9. Waduh, jadi repot ya. Siapa sih yang bikin gara-gara?

Eksperimen heartbeat ditambahkan oleh Robin Seggelmen, seorang programmer asal Jerman, pada tahun 2011, dan dirilis

ke publik pada tahun 2012. Namun ia menyangkal kelemahan itu dilakukan secara sengaja. Kode itu pun lolos dari validasi

yang dilakukan Dr Stephen Henson yang merupakan salah satu anggota inti OpenSSL Foundation.

10. Tapi untung ada yang nemuin. Eh, yang nemuin sapa sih?

Dia adalah Neel Mehta, salah satu anggota Google Security. Atas jasanya tersebut, dia mendapatkan uang sebesar US$ 15

ribu dari Internet Bug Bounty. Namun oleh Neel, uang itu langsung disumbangkan kepada yayasan The Freedom of Press

Foundation yang bergerak di bidang keamanan komunikasi digital