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

**Apa itu Heartbleed?**

Perlu diketahui bahwa Heartbleed bukanlah virus. Heartbleed adalah celah keamanan di salah satu ekstensi OpenSSL yang disebut Heartbeat. Celah keamanan ini memungkinkan attacker untuk membaca memory dari server yang diproteksi oleh OpenSSL. Hasilnya mereka bisa mencuri password, username, dan informasi sensitif lainnya.

**Kapan Heartbleed Pertama Kali Muncul?**

Karena Heartbleed merupakan bug di ekstensi Heartbeat, maka bug ini 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. Heartbleed 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.

**Seberapa Luas Penyebaran Heartbleed**

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 lainnya juga tidak terhindarkan dari Heartbleed ini. Beruntung sudah mulai banyak pengelola website yang mengupdate OpenSSL di server mereka sehingga tidak perlu khawatir dengan Heartbleed lagi.

**Cara Mengetahui Website yang Terkena Heartbleed**

**Dari sisi pengguna**

Kamu bisa melakukan pengecekan dengan menggunakan Heartbleed Test dari [Filippo](https://filippo.io/Heartbleed/)ataupun dari [McAfee](http://tif.mcafee.com/heartbleedtest). Masukkan saja URL website yang ingin kamu cek. Jika hasilnya vulnerable maka website tersebut masih belum kebal terhadap Heartbleed. Kamu juga bisa menggunakan [addon browser](http://forum.winpoin.com/diskusi-ekstensi-warn-heartbleed-browser) untuk semakin memudahkan melihat apakah website yang kamu kunjungi sudah kebal terhadap Heartbleed atau belum.

**Dari sisi pengelola website**

Silahkan cek versi OpenSSL di server yang kamu gunakan. Jika versi OpenSSL di server kamu adalah 1.0.1 hingga 1.0.1f, maka server kamu belum kebal terhadap Heartbleed.

**Cara Mengatasi Heartbleed**

**Bagi pengguna**

Beberapa orang menyarankan kamu untuk segera mengganti password setelah Heartbleed ditemukan. Hal ini salah dan kurang tepat! Jangan buru-buru mengganti password sebelum website tersebut kebal terhadap Heartbleed. Jika situs yang kamu gunakan belum kebal terhadap Heartbleed, tunggu dulu hingga si pengelola website melakukan patch terhadap OpenSSL di servernya. Setelah situs tersebut kebal terhadap Heartbleed, barulah ganti password kamu.

Mengganti password saat situs tersebut belum kebal terhadap Heartbleed cukup berbahaya. Si attacker masih bisa mencuri lagi detail password baru yang kamu masukkan. Mereka baru tidak bisa mengambil detail password baru kamu jika OpenSSL di server situs tersebut sudah di patch oleh pengelolanya.

Solusi lainnya adalah dengan menggunakan satu password untuk satu situs. Dengan begitu jika kamu tanpa sengaja menggunakan layanan website yang belum kebal terhadap Heartbleed, dan si attacker berhasil mengambil detail akun kamu, maka dia tidak bisa membobol akun kamu di layanan-layanan lainnya. Tentu saja untuk memudahkan kamu dalam mengingat password, kamu bisa menggunakan Password Manager seperti [KeePass](http://keepass.info/) maupun [LastPass](https://lastpass.com/).

Untuk semakin mengamankan akun kamu, pastikan kamu 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 dia sudah mengantongi username dan passwordnya.

**Bagi Pengelola Situs**

Jika server kamu 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 kamu gunakan di server kamu. Jangan lupa juga ingatkan user untuk mengganti password mereka. Kamu juga bisa “sedikit memaksa” dengan melakukan reset password semua user. Ini semua demi keamanan pengguna layanan di situs kamu.

**Beberapa Mitos yang Salah Seputar Heartbleed**

* **Heartbleed itu virus:** Salah. Heartbleed bukanlah virus. Dia adalah bug di ekstensi Heartbeat OpenSSL versi 1.0.1 sampai 1.0.1f
* **Segera update antivirus biar kebal Heartbleed:** Salah. Update antivirus tidak akan berpengaruh terhadap kebal atau tidaknya PC terhadap Heartbleed. Sekali lagi Heartbleed bukanlah virus dan dia tidak menyebar atau menginfeksi PC kita.
* **Jika situs yang kamu gunakan belum kebal terhadap Heartbleed, segera ganti password kamu:** Salah. Ganti password kamu setelah situs tersebut di patch 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 kamu.

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

# Heartbleed Bug: Definisi, Titik Rentan, dan Cara Penanggulangannya

Heartbleed Bug adalah sebuah kerentanan kritis yang ada dalam library perangkat lunak kriptografik populer, OpenSSL. Titik Rentan ini memungkinkan pencurian informasi yang sewajarnya dilindungi oleh enkripsi SSL/TLS sebagai enkripsi pengamanan internet. SSL/TLS menyajikan fungsi keamanan dan privasi di internet bagi sejumlah aplikasi seperti website, email, pesan instan (IM), dan beberapa virtual private networks (VPN).

*Bug Heartbleed memampukan siapa saja untuk membaca memori sistem yang dilindungi oleh versi rentan software OpenSSL.*

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 gilirannya, para penyerang (attacker) bisa:  
– mencuri dengar lalu lintas komunikasi,  
– mencuri data secara langsung dari server dan user,  
– serta menyamar sebagai penyedia layanan maupun pengguna.

**Daftar Isi**[[buka](http://ekajogja.com/heartbleed-bug-definisi-titik-rentan-dan-cara-penanggulangannya/)]

### Apa saja informasi yang bocor akibat Heartbleed Bug?

Kami (baca: [Codenomicon](http://www.codenomicon.com/)) telah menguji beberapa layanan kami dengan menggunakan sudut pandang penyerang (cracker). Kami menyerang sistem layanan kami dari sisi luar tanpa meninggalkan jejak sama sekali. Tanpa memanfaatkan informasi maupun kredensial khusus, kami mampu mencuri kunci-kunci rahasia yang dipakai untuk sertifikat X.509, nama dan password pengguna,instant messages, surel, serta informasi dan dokumen-dokumen bisnis penting yang ada pada layanan kami.

### Bagaimana menghentikan kebocoran dan menanggulangi dampak Bug Heartbleed?

Selama versi rentan OpenSSL masih dipergunakan, ia tetap bisa disalahgunakan. Saat ini, [Fixed OpenSSL](http://www.openssl.org/news/secadv_20140407.txt) 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](http://cve.mitre.org/).

#### 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)

#### Siapa yang menemukan Heartbleed Bug?

Bug ini ditemukan secara independen oleh sebuah tim security engineer (Riku, Antti, dan Matti) dari Codenomicon dan Neel Mehta dari Google Security, yang pertamakali melaporkannya pada tim OpenSSL.

#### Dimana mencari informasi selengkapnya?

Tulisan ini (versi asli di heartbleed.com – red.) diterbitkan sebagai tindak lanjut dari laporan OpenSSL sejak kerentanan ini dipublikasikan pada 7 April 2014. OpenSSL telah membuat pernyataan di [https://www.openssl.org/news/secadv\_20140407.txt](http://www.openssl.org/news/secadv_20140407.txt). NCSC-FI merilis pemberitahuan di[https://www.cert.fi/en/reports/2014/vulnerability788210.html](http://www.cert.fi/en/reports/2014/vulnerability788210.html). Para penyediaoperating system distribution, pemilik layanan internet, paket software, dll. yang terkena dampak barangkali akan mempublikasikan pernyataan mereka secara terpisah.

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

Sebelumnya perlu diketahui heartbleed bukanlah virus. Heartbleed adalah celah keamanan pada salah satu ekstensi OpenSSl yang disebut heartbeat. Celah keamanan memumngkinkan *attacker*(hacker/cracker) untuk membaca memori dari server yang diproteksi oleh OpenSSL. Deangan celah keamanan tersebut para attacker dapat mencuri data penting yang disimpan deserver seperti password, username, dan informasi penting lainnya.

SSL adalah standar keamanan yang akan mengenkripsi teks (seperti username dan password) yang user kirim via browser.   
OpenSSL adalah salah satu teknik SSL tersebut. Dinamakan “open” karena memang bersifat open source.

Heartbeat adalah salah satu fitur OpenSSL yang diperkenalkan tahun 2012. Tujuan heartbeat adalah mengecek apakah komputer user masih terhubung ke sebuah server.

**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.

**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**

User dapat mengetahui website yang terkena heartbleed, menggunakan Heartbleed Test dari [Filippo](https://filippo.io/Heartbleed/) ataupun dari [McAfee](http://tif.mcafee.com/heartbleedtest). Dengan cara memasukkan URL website yang dicurigai. jika hasilnya vulnerable maka website tersebut masih belum kebal terhadap Heartbleed. user juga bisa menggunakan [addon browser](http://forum.winpoin.com/diskusi-ekstensi-warn-heartbleed-browser) untuk semakin memudahkan melihat apakah website yang user kunjungi sudah kebal terhadap Heartbleed atau belum.

**Dari sisi pengelola website**

Untuk para pengelola website dapat melakukan pengecekkan versi OpenSSL di server yang gunakan. 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**

Bagi pengguna setelah mengecek bahwa website tersebut terkena heartbleed, dapat menghubungi pengelola website tersebut. User dapat menanyakan kapan akan ditutup bug tersebut. Atau jika pengelola tersebut belum mengetahuinya , user dapat mengingatkan agar pengelola segera menambal bug tersebut.

Ada baiknya gunakan password yang berbeda disetiap website yang tidak kebal pada heartbleed , hal ini mengurangi resiko kehilangan data yang lebih besar.

Untuk semakin mengamankan akun , ada baiknya 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 dia sudah mengantongi username dan passwordnya.

**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 website<https://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".

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

### Apa itu Heartbleed Bug?

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. OpenSSL kemudian dikembangkan secara Open Source untuk membantu proses pengamanan protokol di interner. OpenSSL diterapkan pada akhir tahun 1998 silam .  
  
Berdasarkan data yang diperoleh dari berbagai sumber dan Mashable, **Heartbleed adalah sebuah bug yang ada di dalam kriptografi OpenSSL**. Kriptografi itu digambarkan menyerupai grafik detak jantung pada alat monitoring detak jantung.  
  
Bug itu membuka celah agar setiap orang di internet mengakses lalu lintas memori yang berlangsung dari server ke client, begitu pula sebaliknya. Akses dari lalu lintas memori itu bisa memberikan kesempatan kepada hacker agar bisa memperoleh kunci masuk dan mengakses ke dalam sebuah layanan milik orang lain, setelah masuk melalui akses yang berhasil diekspos, hacker dapat dengan mudah mengambil berbagai informasi pribadi seperti username, password, data kartu kredit maupun data penting lainnya.

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

Apa itu Heartbleed bug?  
  
Bug ini memanfaatkan fungsi Heartbeat pada OpenSSL dan si hacker bisa mendapatkan isi dari memory pada server yang besarnya sampai 64KB. Ini bisa dilakukan berulang – ulang karena tidak bisa dideteksi kalau sedang diserang. Jadi dengan perlahan tapi pasti seluruh isi dari RAM server akan bisa diketahui rahasianya.  
  
Kenapa diberi nama Heartbleed?  
  
Karena bug ini berasal dari implementasi protokol heartbeat (RFC6520) TLS/DTLS (Transport Layer Security Protocols). Kalau protokol “denyut jantung” ini dieksploitasi maka akan membocorkan isi memori dari server ke klien. Karena itu laha namanya kalau diartikan adalah “pendarahan jantung”.  
  
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.