http://www.bppk.kemenkeu.go.id/publikasi/artikel/419-artikel-teknologi-informasi/20804-heartbleed-bug-hati-luka-pembawa-bencana

[Heartbleed Bug](http://www.bppk.kemenkeu.go.id/publikasi/artikel/419-artikel-teknologi-informasi/20804-heartbleed-bug-hati-luka-pembawa-bencana)

Beberapa waktu belakangan ini jagad dunia maya digemparkan dengan ditemukannya celah keamanan pada OpenSSL yang dinamakan dengan *Heartbleed*. Celah keamanan ini sangat berbahaya sehingga setiap pengguna maupun pengelola website dilarang keras untuk mengabaikan celah keamanan yang satu ini. Karena tingkat resikonya yang teramat tinggi, celah keamanan ini bahkan disebut-sebut sebagai bencana terbesar yang pernah terjadi sepanjang sejarah internet berdiri.

Klaim tersebut tidaklah berlebihan mengingat banyaknya situs dan layanan *online* lainnya yang menggunakan OpenSSL untuk mengamankan aliran atau transfer data dari web server ke komputer pengguna. Tidak tanggung-tanggung, website sekelas Facebook, Google, Yahoo, Dropbox, Instagram, Flickr, Pinterest dan berbagai website populer lainnya tidak luput dari bencana ini. Diperkirakan ada sekitar 2/3 website di seluruh dunia terkena dampak dari celah keamanan ini.

Celah keamanan ini pertama kali di deteksi pada tanggal 7 April 2014 oleh Neel Mehta yang merupakan anggota tim dari Google Security dan dipublikasikan pada CVE (*Common Vulnerability and Exposure*) nomor CVE-2014-0160 (<http://www.openssl.org/news/secadv_20140407.txt>). Letak permasalahannya terdapat pada salah satu ektensi dari OpenSSL yang bernama *heartbeat* dimana celah keamanan pada ekstensi tersebut memungkinkan seorang peretas melakukan *dump* data yang tersimpan dalam memori server dan mendekrip data tersebut. Setelah data berhasil didekrip peretas akan dapat dengan mudah membaca seluruh data tersebut. Celakanya, data yang di-*dump* oleh sang*attacker* umumnya merupakan *username* dan *password* pengguna yang terkoneksi dengan webserver. Dan yang lebih mengejutkan adalah, ternyata celah keamanan ini telah ada sejak ekstensi *hearbeat*ini pertama kali di rilis pada tahun 2011 dan baru terdeteksi pada april 2014. Maka tidak berlebihan apabila celah kemanan ini disebut sebagai bencana terbesar sepanjang sejarah *World Wide Web*(baca : internet).

OpenSSL sendiri merupakan sebuah modul perangkat lunak kriptografi yang dijalankan pada protokol jaringan *Secure Socket Layer* (SSL) dan *Transport Layer Security* (TLS). Fungsi utama dari OpenSSL adalah mengamankan aliran data dari komputer pengguna ke server yang dituju dengan cara melakukan enkripsi dan dekripsi aliran data yang mengalir dari komputer pengguna ke server yang dituju. Dengan menggunakan OpenSSL, data yang mengalir akan lebih sulit untuk disadap (*sniff)* dan seandainya seorang peretas berhasil melakukan penyadapan terhadap data yang mengalir tersebut, tentu saja data tersebut tidak akan dapat dibaca karena data yang disadap tersebut masih dalam bentuk *hash*.

Selain pada web server, celah keamanan ini juga terdapat pada berbagai layanan lainnya yang menggunakan OpenSSL untuk melakukan enkripsi dan dekripsi data. Tercatat celah keamanan ini juga terdapat pada jutaan *smartphone* dengan sistem operasi Android. Celah keamanan ini juga terdapat pada perangkat jaringan lainnya seperti *switch*, hub, *router*, ip-*phone*, serta perangkat *video conference*  dengan merk Cisco dan Juniper. Celah keamanan ini berhasil memaksa para vendor tersebut untuk segera melakukan perbaikan dan merilis *patch* untuk jutaan perangkat mereka yang tersebar diseluruh dunia.

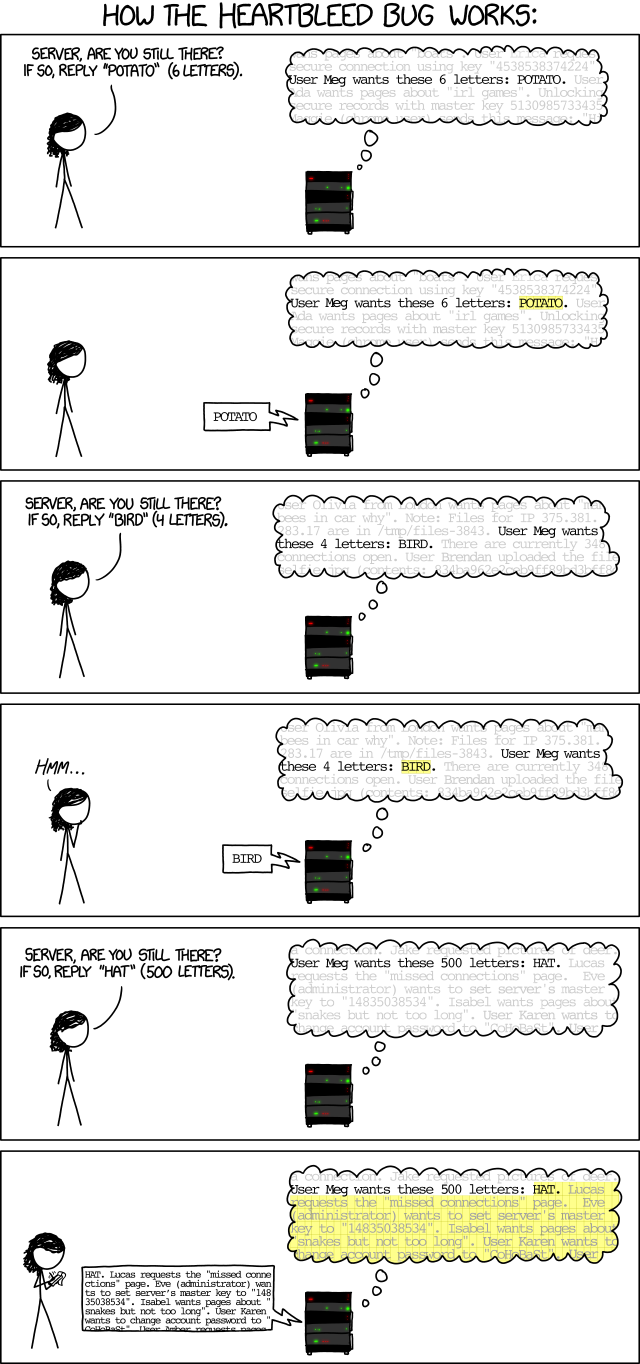
Cara Kerja Heartbleed Bugs

Pada komunkasi data dengan menggunakan protokol jaringan SSL, protokol tersebut selalu menyertakan opsi *heartbeat* yang berfungsi untuk memberikan pesan kepada server yang bertujuan untuk memberitahu server bahwa komputer pengguna masih dalam keadaan aktif dan terknoneksi melalui jaringan SSL ke server tersebut. Opsi ini sangat berguna karena sebagian besar internet*router* akan segera memutuskan koneksi SSL apabila tidak ada aktifitas dari user dalam waktu yang lama.

Pesan yang dikirim ke server terdiri dari tiga bagian yaitu *acknowledgement message*, *random message,* dan jumlah karakter dari *random message* tersebut. Setelah pesan tersebut sampai ke server, server akan segera mengirimkan pesan balasan kepada user berupa *acknowledgement message* dan *random message* dengan jumlah karakter sesuai dengan yang dikirimkan oleh user.

Letak permasalahannya adalah, server tidak melakukan validasi jumlah karakter dari *random message* yang disebutkan oleh user. Sehingga server akan selalu memberikan respon sesuai dengan jumlah karakter yang disebutkan oleh user tanpa melakukan validasi jumlah karakter dari *random message*. Hal ini dimanfaatkan oleh para *malicous user* untuk mendapatkan data yang terdapat*random access memory* (RAM) server dengan cara mengirimkan jumlah karakter palsu ke server dan server pun akan dengan sukarela mengirimkan seluruh data yang terdapat dalam RAM kepada*malicious user*.

Untuk dapat lebih memahami cara kerja dari *Heartbleed Bugs*, perhatikan ilustrasi cara kerjanya pada Gambar 1.



Gambar 1 : Ilustrasi Cara Kerja *Heartbleed Bugs (*Sumber Gambar : [http://imgs.xkcd.com](http://imgs.xkcd.com/))

Mendeteksi *Heartbleed Bugs*

Bagaimanakah cara mendeteksi suatu website atau aplikasi berbasis web memiliki celah kemanan ini? Untuk mengetahui apakah suatu website atau aplikasi berbasis web memiliki celah keamanan ini dapat dilakukan dengan menggunakan layanan online yang telah disediakan oleh McAfee (<http://tif.mcafee.com/heartbleedtest>) secara cuma-cuma. Anda hanya perlu memasukan alamat website yang ingin anda cek pada kolom yang tersedia kemudia tekan tombol scan, McAffe akan segera memeriksa website tersebut dan dalam hitungan menit hasil pemeriksaan dari McAffe akan segera muncul dilayar monitor anda. Yang perlu dicatat disini adalah, layanan tersebut hanya dapat memeriksa website-website yang terletak pada jaringan internet dan bukan pada website yang terletak pada jaringan internal atau intranet. Untuk melakukan pengecekan pada website atau aplikasi yang terletak pada jaringan internal dapat dilakukan dengan cara memeriksa versi OpenSSL yang digunakan. Apabila versi OpenSSL yang digunakan pada webserver adalah versi 1.0.1 hingga 1.0.1f, maka sudah dapat dipastikan server tersebut memiliki celah keamanan Heartbleed.

Sedangkan untuk mendeteksi keberadaan *heartbleed* pada *smartphone* dengan sistem operasi android, dapat dilakukan dengan menggunakan aplikasi bernama *Heartbleed Detector* yang dibuat oleh sebuah perusahaan antivirus bernama Lookout. Aplikasi ini dapat di unduh secara gratis pada Google Play Store. Hampir dapat dipastikan sebagian besar *smartphone* dengan sistem operasi android versi Jelly Bean memiliki celah kemanan *heartbleed* dan celah tersebut berhasil di deteksi oleh aplikasi *Heartbleed Detector*. Namun patut dicatat bahwa aplikasi *Heartbleed Detector* hanya akan melakukan pendeteksian celah keamanan *heartbleed* dan tidak melakukan perbaikan celah keamanan tersebut.

Mengatasi *Heartbleed*

Bagaimana cara mengatasi celah keamanan ini? Celah keamanan ini dapat diatasi dengan melakukan-update OpenSSL dengan versi yang terbaru. Pada versi OpenSSL yang terbaru, celah keamanan ini telah berhasil diperbaiki dan dapat sudah dapat dipastikan pada versi ini telah kebal dari peretas yang melakukan serangan dengan memanfaatkan *Heartbleed Bugs*.

Mengatasi celah keamanan *heartbleed* dengan melakukan *upgrade* OpenSSL hanya dapat dilakukan oleh para pengelola website bukan para pengguna/*client* dari website tersebut. Yang dapat dilakukan oleh pengguna/client dari website yang memiliki celah keamanan *heartbleed* adalah mengaktifkan*Two-Factor Authentication* jika fitur tersebut tersedia dalam situs yang anda gunakan. Pada saat ini berbagai situs populer seperti Google Mail, Facebook, Yahoo dan lain sebagainya telah menerapkan teknologi ini untuk mengamankan akun para penggunanya. Teknologi *Two-Factor Authentication*dapat mencegah para peretas untuk masuk kedalam akun anda walaupun peretas tersebut telah mengantongi *username* dan *password* akun anda. Selain itu, segera ganti *password* anda setelah pengelola website melakukan penambalan celah kemanan *heartbleed* untuk mencegah terjadinya hal-hal yang tidak diinginkan.

Mitos

Karena kehadirannya yang berhasil menggemparkan dunia internet, beredar berbagai macam mitos yang salah dan berlebihan terhadap celah kemananan ini. Mitos-mitos tersebut antara lain :

*Heartbleed* adalah virus

Mitos tersebut sudah dapat dipastikan tidak valid. *Heartbleed* bukanlah virus. *Heartbleed*merupakan celah keamanan pada OpenSSL yang muncul karena terdapat kesalahan pada penulisan kode program dalam protokol enkripsi *open-source* yang banyak digunakan oleh situs-situs diseluruh dunia.

Update antivirus agar kebal dari *Heartbleed*

Mitos ini sudah dapat dipastikan tidak valid. Melakukan update antivirus tidak akan berpengaruh terhadap kebal atau tidaknya perangkat komputer dari celah keamanan *Heartbleed*. Yang perlu ditekankan disini adalah *Heartbleed* bukan virus, tidak menyebar dan tidak menginfeksi perangkat komputer lainnya baik via jaringan komputer maupun media penyimpanan.

Segera ganti *password* apabila situs yang Anda gunakan belum kebal dari *Heartbleed*

Mitos ini sangat tidak benar. Yang benar adalah segera ganti *password* apabila situs yang Anda gunakan telah melakukan penambalan terhadap celah keamanan *Heartbleed*. Apabila Anda melakukan perubahan password pada saat celah keamanan tersebut belum ditambal, sama saja memberikan kesempatan kepada peretas untuk mengetahui password baru Anda.

Peretas dapat memanfaatkan *Heartbleed* untuk mengontrol berbagai *smartphone*

Mitos ini juga salah. Sampai dengan saat ini celah kemanan ini hanya dapat dimanfaatkan untuk mengambil data yang tersimpan dalam memori sebuah *smartphone* yang belum melakukan penambalan terhadap celah kemanan *Heartbleed*.

Celah keamanan ini hanya terjadi pada sistem operasi Android versi Jelly Bean (4.1.1) sedangkan untuk smartphone dengan sistem operasi iOS dan Windows Phone dapat dipastikan kebal dari celah keamanan ini karena dalam sistem operasi iOS dan Windows Phone  tidak menggunakan OpenSSL.

Windows XP rentan dari Heartbleed karena sudah tidak di support oleh Microsoft

Mitos ini sudah dapat dipastikan salah. Berdasarkan informasi yang terdapat dapat dalam blog developer Microsoft, perusahaan tersebut tidak menggunakan OpenSSL dalam pembangunan dan pengembangan sistem operasi Microsoft Windows XP dan seluruh versi sistem operasi Windows lainnya termasuk sistem operasi untuk *smartphone* Windows Phone

Dalam proses pembangunan dan pengembangan sistem operasi Windows, Microsoft menggunakan komponen kriptografi yang mereka ciptakan sendiri yaitu Secure Channel sehingga dapat dipastikan seluruh product dari Microsoft mulai dari sistem operasi sampai dengan layanan lainnya seperti outlook, skype dan lain sebagainya kebal dari celah kemananan *Heartbleed*.

Semua layanan internet banking rentan terhadap *Heartbleed*

Mitos ini tidak dapat pastikan kebenarannya karena sebagian besar layanan internet *banking* dan berbagai situs jual beli populer tidak menggunakan OpenSSL sehingga layanan-layanan tersebut tidak terkena dampak dari celah kemanan *Heartbleed*

NSA memanfaatkan Heartbleed sejak lama untuk memata-matai kita

Beredar isu yang mengatakan bahwa agen intelijen Amerika (NSA) telah mengetahui celah kemanan tersebut sejak lama, namun memilih diam dan memanfaatkan celah kemanan tersebut untuk melakukan kegiatan mata-mata.Isu tersebut telah dibantah oleh NSA dan mengatakan bahwa pihaknya tidak menggunakan celah kemanan tersebut untuk kegiatan mata-mata dan mengaku baru mengetahui celah tersebut setelah diumumkan.

Dengan terungkapnya celah keamanan yang terdapat dalam OpenSSL telah menjadi bukti nyata bahwa *vulnerability assessment* merupakan proses yang wajib dilakukan oleh para pengelola IT di seluruh institusi baik institusi pemerintah maupun institusi swasta. Pada kebanyakan institusi, proses*vulnerability assessment*hanya dilakukan sebelum melakukan implementasi suatu sistem informasi dan jarang sekali ada institusi yang melaksanakan proses *vulnerability assessment* pasca implementasi suatu sistem informasi dengan berbagai macam alasan.

Berkaca dari kasus celah keamanan *heartbleed* pada OpenSSL yang  baru ditemukan setelah beberapa tahun dirilis, maka dapat disimpulkan bahwa proses *vulnerability assessment* harus dilakukan baik sebelum implementasi sistem informasi dan sesudah implementasi sistem informasi. Proses *vulnerability assessment* juga harus dilakukan secara berkala. Hal ini tidaklah berlebihan mengingat saat ini perkembangan teknologi informasi dan komunikasi sangat pesat yang sudah pasti kejahatan dengan menggunakan teknologi informasi juga akan meningkat pesat karena perkembangan teknologi akan selalu berbanding lurus dengan meningkatnya angka kejahatan dengan memanfaatkan teknologi.

Selain melaksanakan proses *vulnerability assessment*, proses pembaruan (*update*) dan penggandaan (*backup*) sistem juga wajib hukumnya untuk dilakukan. Umumnya dalam pembaruan suatu sistem terdapat perbaikan terhadap berbagai macam kesalahan atau *error* maupun perbaikan dalam rangka untuk menutup celah keamanan. Sedangkan proses penggandaan diperlukan untuk mencegah terjadinya hal-hal yang tidak diinginkan.