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.

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.