Surat Berita Bulanan berkenaan Kesedaran Keselamatan Untuk Pengguna Komputer

OUCH!

DALAM ISU KALI INI...

- Apa itu Heartbleed?
- Apa Yang Perlu Saya Lakukan?
- Berhati-hati dengan Serangan Phishing

Heartbleed – Mengapa Kita Perlu Ambil Peduli?

Pengenalan

Pada tanggal 7 April hari Isnin, satu kelemahan yang serius telah ditemui dalam salah satu pelaksanaan protokol SSL paling popular yang dikenali sebagai OpenSSL. SSL merupakan protokol keselamatan yang paling penting di internet. SSL bukan sahaja mengenkripsi komunikasi dalam talian, tetapi ia juga memastikan anda menyelusuri laman sesawang yang sah ketika membeli atau membuat perbankan dalam talian. Dalam keluaran ini, kami akan memberi gambaran mudah dan menerangkan erti kelemahan ini kepada anda serta apa yang perlu anda lakukan untuk melindungi diri anda.

Editor Jemputan

Jake Williams (@MalwareJake; malwarejake.blogspot.com) merupakan Ketua Ahli Sains di CSRgroup Computer Security Consultants. Beliau juga merupakan penulis bersama kursus Memory Forensics (FOR526) and Malware Reverse Engineering (FOR610) di SANS.

Apa itu Heartbleed?

Kelemahan yang disebabkan oleh Heartbleed membenarkan penggodam membuat sambungan kepada pelayan sesawang dan menuai maklumat sensitif yang mungkin mengandungi log masuk dan kata laluan anda. Jika penyerang mampu berbuat demikian, mereka boleh menggunakan maklumat tersebut untuk masuk ke mana-mana akaun anda dengan menggunakan nama pengguna dan kata laluan yang sama. Walaupun kelemahan ini telah wujud sejak dua tahun yang lalu, ia hanya ditemui dan dihebahkan kepada umum pada 7 April. Heartbleed tidak menjejaskan komputer Windows atau Mac; ia menjejaskan laman sesawang yang anda gunakan di internet, seperti Facebook dan Gmail. Lebih mengelirukan, tidak semua laman sesawang di internet akan terjejas, tetapi kebanyakkannya akan merasai impaknya. Anda boleh menyemak sama ada laman sesawang yang sedang atau pernah anda gunakan mempunyai kelemahan tersebut dengan menggunakan alat menyemak yang dinamakan Lastpass di laman https://lastpass.com/heartbleed/.

Apa Yang Perlu Saya Lakukan?

Ada beberapa langkah yang boleh diambil untuk melindungi diri anda. Langkah ini bukan sahaja dapat membantu melindungi diri anda daripada kelemahan Heartbleed, tetapi ia juga boleh membantu melindungi dan menentang serangan-serangan yang lain kelak:

- Pertama, tukar kata laluan laman sesawang yang anda pasti pernah mengalami kelemahan ini dan telah membuat tampalan, bermula dengan akaun anda yang paling penting. Jika anda tidak pasti, terus tukar kata laluan anda. Ini merupakan masa yang sesuai untuk mengemas kini kata laluan dan mempertingkatkan keselamatan dalam talian anda.
- Semasa mengemaskini kata laluan, pastikan anda menggunakan kata laluan yang teguh dan sukar diduga. Jika laman sesawang tersebut disokong oleh sesuatu yang dipanggil pengesahan dua faktor, aktifkannya. Langkah tambahan ini dapat membantu meningkatkan keselamatan akaun dalam talian anda.
- Pastikan anda menggunakan kata laluan yang unik dan berbeza untuk setiap akaun dalam talian anda. Dengan cara

Heartbleed – Mengapa Kita Perlu Ambil Peduli?

itu, jika satu laman sesawang digodam, akaun-akaun yang lain masih selamat. Anda menghadapi kesukaran mengingati kesemua kata laluan anda? Tahniah, ini bermakna anda menggunakan kata laluan yang teguh. Kami menasihatkan anda mengambil peluang ini untuk mula menggunakan pengurus kata laluan yang berupaya menyimpan kesemua kata laluan anda dengan selamat. Ini merupakan cara terbaik yang bukan sahaja boleh memudahkan aktiviti dalam talian anda, malahan menjadikannya lebih selamat.

- Jangan lupa klien e-mel anda. Jika klien e-mel anda, seperti Outlook atau Apple Mail, menggunakan SSL untuk berhubung dengan pelayan mel anda, anda mungkin perlu menukar kata laluan tersebut.

Jika anda memerlukan maklumat lanjut tentang langkah-langkah di atas, sila lihat bahagian Sumber di akhir surat berita ini.

Cara terbaik untuk melindungi diri anda adalah dengan menukar kata laluan pada akaun utama dan pastikan setiap kata laluan tersebut teguh dan unik.

Berhati-hati dengan Serangan Phishing

Malangnya, penjahat cekap mengambil peluang. Berita mengenai Heartbleed telah tersebar luas dan ramai telah pun mengetahuinya, termasuklah diri anda. Oleh itu, mereka akan mengarang e-mel yang kelihatan seperti ianya berasal daripada laman sesawang yang sah yang sering anda gunakan(seperti perbankan dalam talian atau kedai dalam talian). Mereka mungkin juga menyamar sebagai syarikat keselamatan yang menawarkan alat percuma untuk mengesan kelemahan akibat Heartbleed.

Taktik ini (dikenali sebagai phishing) bukanlah baharu. Penyerang akan cuba untuk memperdayakan anda untuk menekan pautan yang membawa anda ke laman sesawang yang berniat jahat atau cuba memperdayakan anda untuk membuka lampiran yang telah dijangkiti. Jika anda menjadi mangsa kepada serangan seperti ini, komputer anda boleh dijangkiti. Sebaliknya jika anda perlu untuk menukar kata laluan, anda hanya perlu taip nama laman sesawang tersebut (sering dipanggil URL) ke dalam pelayar anda dan tukar kata laluan tersebut secara dalam talian. Dengan cara itu, anda tahu anda sedang menggunakan laman sesawang yang sah.

Burimet

Which Sites Are Vulnerable:	https://lastpass.com/heartbleed/
OUCH! Passwords:	http://www.securingthehuman.org/ouch/2013#may2013
OUCH! Password Managers:	http://www.securingthehuman.org/ouch/2013#october2013
OUCH! Two-Step Verification:	http://www.securingthehuman.org/ouch/2013#august2013
OUCH! Phishing:	http://www.securingthehuman.org/ouch/2013#february2013
Technical Details:	https://www.sans.org/webcasts/openssl-heartbleed-vulnerability-98105

OUCH! diterbitkan oleh program SANS “Securing The Human” dan diedarkan di bawah lesen Creative Commons BY-NC-ND 3.0. Kebenaran diberikan untuk mengedarkan surat berita ini atau mengunakannya dalam mana mana program kesedaran selagi tiada perubahan dibuat kepada kandungan asal.

Editor: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Translated by: Saravanan Kulanthaivelu, Muhamad Hashimi, Rahayu Aziz, and Sheikh Ahmad Raffie