Tisztelt Ügyfelünk!

2014. április elején az SSL technológia használata során alkalmazott OpenSSL kriptográfiai könyvtár TLS "heartbeat" kiterjesztésében biztonsági rést fedeztek fel, mely HEARTBLEED néven vált ismertté (hivatalosan: CVE-2014-0160, http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160). Ez külső felek (adott esetben támadók) számára lehetővé teszi, hogy bizonyos OpenSSL függvénykönyvtár verziókkal védett rendszerek memóriájának egy 64 kilobájtos szeletéhez hozzáférjenek és ezen keresztül adatszivárgás történhessen. A memória szivárgása során kritikus adatok (például felhasználónevek, jelszavak) és az adatforgalom titkosítására használt privát kulcsok is kikerülhetnek anélkül, hogy annak bármilyen nyoma lenne. A biztonsági rés miatt a privát kulcsok kompromittálódhatnak, azok birtokában pedig a szerver-kliens közötti információkhoz a támadók hozzáférhetnek, illetve ha korábbi titkosított kommunikáció rendelkezésükre áll, akkor azt is visszafejthetik. A memóriatartalom szivárgása sessionökön keresztül is átnyúlhat, azaz egy későbbi felhasználó egy korábbi felhasználó után maradt nyomokat is láthatja a szerveren.

A problémát nem az SSL tanúsítvány okozza és nem is a protokollból ered, hanem egy egyedi hibás OpenSSL implementáció eredménye.

Az érintett, sérülékeny OpenSSL verziók:

- teljes OpenSSL 1.0.1 sorozat OpenSSL 1.0.1.f –ig
- OpenSSL 1.0.2 beta1

A javított verzió, mely már tartalmazza a fixet:

OpenSSL 1.0.1g (letöltés: https://www.openssl.org/source)

A BUG által érintett szerverek, szolgáltatások és rendszerek

a. Web szolgáltatások (HTTPS): például Apache, Ngingx vagy bármilyen szerver, amely az érintett OpenSSL függvénykönyvtárat használja

b. Mail szolgáltatások (STARTTLS): titkosított csatornát használó levelező szolgáltatások (IMAPS, POP3S, SMTPS), amely az érintett OpenSSL verziókat használja

c. SSL alapú VPN –ek

d. OpenSSL alapú autentikációs mechanizmusok

e. operációs rendszerek: sérülékeny OpenSSL függvénykönyvtárral kibocsátott operációs rendszerek (ezek későbbi frissítése OpenSSL 1.0.1g –re már megoldja a problémát):

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 (2012.05.10)

OpenBSD 5.4 -> OpenSSL 1.0.1c (2012.05.10)

FreeBSD 10.0 -> OpenSSL 1.0.1e (2013.02.11)

NetBSD 5.0.2 -> OpenSSL 1.0.1e

OpenSUSE 12.2 -> OpenSSL 1.0.1c

A fenti rendszereken kívül természetesen minden olyan szoftver érintett, mely a sérülékeny OpenSSL verziót használja.

Kérjük, hogy a BUG által okozott hiba elhárításához az alábbi SORRENDBEN kövesse a teendőket!

1. Ellenőrizze, hogy szerverén/rendszerén sérülékeny OpenSSL verziót használ-e.

Parancssoros ellenőrzés például Windows esetén:

1. Start > Futtatás > cmd
   (szükség esetén lépjen be az openssl bin könyvtárába)
2. írja be:

   openssl version
3. Ha a visszakapott verziószám az alábbiak egyike, akkor a rendszer ÉRINTETT, frissítés szükséges:

   OpenSSL 1.0.1 - OpenSSL 1.0.1.f

   vagy

   OpenSSL 1.0.2 beta1

Parancssoros ellenőrzés például Linux esetén:

1. Indítson terminált.
2. Írja be:

   openssl version
3. Ha a visszakapott verziószám az alábbiak egyike, akkor a rendszer ÉRINTETT, frissítés szükséges.

   OpenSSL 1.0.1-OpenSSL 1.0.1.f

   vagy

   OpenSSL 1.0.2 beta1

2. Ha nem és/vagy sosem alkalmazta a hibás verziót, úgy szerverén/rendszerén nincsen teendője. Ha igen, úgy változtassa meg az alkalmazott OpenSSL verzióját vagy annak megfelelő paraméterét az alább felsorolt módok egyikével!

a.) frissítse szerverét/szolgáltatását a legújabb OpenSSL verzióval:

OpenSSL 1.0.1g vagy később (letöltés: https://www.openssl.org/source), vagy

b.) térjen vissza az OpenSSL 1.0.0 –hoz (vagy korábbi verzióihoz), vagy

c.) átmeneti megoldásként újrafordíthatja az alkalmazott OpenSSL verziót a DOPENSSL_NO_HEARTBEATS kapcsoló használatával, amennyiben az adott alkalmazási környezet ezt lehetővé teszi.

3. Generáljon új kulcsokat és igényeljen szerverére új SSL tanúsítványokat.

A Netlock SSL tanúsítványait itt rendelheti meg:

Klasszikus SSL tanúsítványok: https://www.netlock.hu/html/ssl/megrendeles.html

Automata SSL tanúsítványok: https://onlinessl.netlock.hu/

4. Az újonnan generált kulccsal és kiadott tanúsítványokkal cserélje le a régi kulcsot és tanúsítványt az érintett rendszerben, annak kezelési útmutatója szerint úgy, hogy már az új kulccsal dolgozzon a rendszer (adott esetben ez a rendszer újraindítását és egyéb lépéseket igényelhet).

Nagyon fontos, hogy ez a lépés csak az 2. és 3. lépés után következhet!

5. Vonja vissza a még érvényben lévő, régi SSL tanúsítványát!

6. Tekintve, hogy a memóriaszivárgás során a HTTPS oldalon/szolgáltatáson keresztül bekért felhasználónév/jelszó párosok is illetéktelen kezekbe kerülhettek, feltétlenül javasoljuk, hogy az OpenSSL verzió frissítése és az új SSL tanúsítvány telepítése után kérje Ügyfeleitől a feléjük nyújtott, szerver alapú szolgáltatás során használt jelszavaik cseréjét is.

A Heartbleed biztonsági hibát nem az SSL tanúsítvány okozza, hanem az OpenSSL egy hibás implementációja, így az incidens sem a Netlock, sem bármely más CA nevéhez nem köthető. Cégünk a szükséges belső biztonsági lépéseket a szolgáltatás védelme érdekében teljeskörűen megtette, saját szervereit, alkalmazásait frissítette, kulcsait újakra cserélte, melyet Ügyfeleinktől is kérünk.

A szolgáltatásunk használatához szükséges ügyféljelszavak cseréje folyamatban van, a tanúsítványcserék elvégzésével és lehetőségeivel kapcsolatban érvényes tanúsítvánnyal rendelkező Ügyfeleink pedig levélben kapnak további tájékoztatást.
