MMXIV. II. ÉVFOLYAM IV. SZÁM

NEMZETBIZTONSÁGI SZEMLE

KÜLÖNLENYOMAT

NEMZETI KÖZSZOLGÁLATI EGYETEM
NEMZETBIZTONSÁGI INTÉZET
BUDAPEST

OPenssl (Heartbleed) sérülékenység avagy a nyílt https

Szabó Tibor[1]

Absztrakt:

Elég nagy visszhangot kapott az internetes sajtóban a közelmúltban nyilvánosságra hozott OpenSSL sérülékenység. Ez annak köszönhető, hogy a mindennapi életünkben biztonságosnak hitt kommunikációnk sérülékenynek bizonyult és ebből kifolyólag féltett személyes adataink és jelszavaink illetéktelen kezébe kerülhettek. Másrészt az váltotta ki a felháborodást, hogy évek óta nem javította ki senki. Cikkemben érintőlegesen ismertetek néhány korábbi, hasonló hibát a Heartbleed mellett, melyek hasonló sajátosságokat mutattak a támadások és a hiba keletkezése kapcsán - elhagyva azokat a technikai részleteket, melyek nem közvetlenül tartoznak a tárgyhoz.

Kulcsszavak: *OpenSSL, memória túlcsordulás, sebezhetőség*

Abstract:

Recently published OpenSSL vulnerability has given quite great echo in the online press. This is due to the fact that the secure communications believed proved vulnerable in our daily lives and therefore precious personal information and passwords may have been accessed by unauthorized parties. On the other hand that have provoked the outrage that no one had been prepared this bug for years. In my article I review some earlier and similar error like Heartbleed, which showed similar characteristics of the attacks and the formation of the failure - leave the technical details that are not directly relevant to the issue.

Keywords: *OpenSSL, SSL/TLS, Heartbleed, Hearbeat, buffer overflow, vulnerability*

[1] *szabo.tibor@nbsz.gov.hu*

Bevezetés

Napjainkban egyre gyakrabban használjuk leveleinken kívül a személyes adataink tárolására is az interneten lévő adatbázisokat, mivel a szolgáltatók – pénzügyi érdekeinknek megfelelően - számunkra egyre több értéknövelt szolgáltatást – köztük a biztonságos hozzáférés és biztonságos tárhely – biztosítanak. A kényelem és gyorsaság mellett a biztonságot megvalósító SSL/TLS kapcsolatot meggyőző alapfeltételnek tekintettük mindmáig.

Elég nagy visszhangot kapott az internetes sajtóban a közelmúltban nyilvánosságra hozott OpenSSL sérülékenység, mely részben annak köszönhető, hogy a mindennapi életünkben biztonságosnak hitt kommunikációnk sérülékenynek bizonyult és ebből kifolyólag féltett személyes adataink és jelszavaink illetéktelen kezébe kerülhettek. Másrészt az váltotta ki a felháborodást, hogy évek óta nem javította ki senki, ami felveti a szándékosságot. Cikkemben érintőlegesen ismertetek néhány korábbi, hasonló hibát a Heartbleed mellett, melyek hasonló sajátosságokat mutattak a támadások és a hiba keletkezése kapcsán - elhagyva azokat a technikai részleteket, melyek nem közvetlenül tartoznak a tárgyhoz.

1. AZ OPENSSL

Az OpenSSL projekt[2] (mely önkéntesek világméretű közösségére támaszkodik) megalakulásakor azt a célt tűzte maga elé, hogy egy teljes értékű, nyílt forráskódú és kereskedelmi színvonalú eszköztárat biztosítson az SSL (Secure Sockets Layer) és a TLS[3] (Transport Layer Security) hálózatbiztonsági protokollok kiszolgálására és mindemellett általános célú titkosítási funkciók megvalósítására. Az eszköztár alapja C programnyelven íródott, melynek első hivatalos verzióját (OpenSSL 0.91c[4]) 1998. december 23-án bocsátották ki, ami az SSLeay[5] őscsomagon alapszik.

---

[2] *Welcome to the OpenSSL Project: https://www.openssl.org/ (2014.05.05.)*

[3] *Az OSI szállítási rétegben működő hálózatbiztonsági protokollok a hagyományos kommunikációs csatornában egy titkosított információátvitelt biztosítanak úgy, hogy azokat harmadik fél ne tudja értelmezni és észrevétlenül módosítani.*

[4] *Project Newsflash!:https://www.openssl.org/news/ (2014.05.05.)*

[5] *Az OpenSSL őscsomagja, melynek fejlesztését Eric Andrew Young és Tim J. Hudson 1998. december 17-én befejezett, mivel az RSA Security számára kezdtek dolgozni. OpenSSL: http://en.wikipedia.org/wiki/OpenSSL (2014.05.05.)*

1. ábra: OpenSSl logója[6]

Az OpenSSL egy sokoldalú. sokféle célra felhasználható programcsomag, mely a következő részekre bontható:

- parancssori alkalmazás (openssl): a titkosítási feladatok végrehajtásának széles körét biztosítja, pl.:
  - a tanúsítványok[7] és a hozzá kapcsolódó állományok létrehozását és életciklus kezelését,
  - a szerver és a kliens közötti SSL/TLS kapcsolat tesztelését,
  - adatállományok titkosítását.
- libcrypto függvénykönyvtár: aszimmetrikus és szimmetrikus kulcsú titkosításhoz és ún. hash funkciókhoz biztosít függvényeket.
- libssl függvénykönyvtár: a libcrypto titkosítási rutinjait használva megvalósítja az SSLv2/v3 és TLSv1 protokollok működését és létrehoz egy programozói interfészt (API - Application Programming Interface) az alkalmazások számára.

Érdemes kihangsúlyozni, hogy egy adott tanúsítvány bármelyik számítógépen létrehozható és bármely más számítástechnikai eszköz(ök)re telepíthető hálózati kapcsolat biztonságának növelése érdekében.

A teljesség igénye nélkül néhány példát érdemes felsorolni, ahol tanúsítványokra van szükség[8]:

- bármely https kapcsolat esetén, amikor egy felhasználó felkapcsolódik egy szerverre és bizonyos szeretne lenni abban, hogy azt valójában egy olyan szervezet/személy üzemelteti, aki birtokolja az adott domain nevet.
- https kapcsolat esetén, amikor hitelesíteni kell a felhasználót a szerver felé.
- szoftver komponensek esetén, ahol bizonyítani kell, hogy egy megbízható szervezet/személy készítette a program kódot.

---

[6] *Project Newsflash!:https://www.openssl.org/news/ (2014.05.05.)*

[7] *Elektronikusan aláírt nyilvános kulcs.*

[8] *Certificate Lifecycle: http://wiki.openssl.org/index.php/Certificate_Lifecycle (2014.05.05.)*

- digitálisan aláírt elektronikus levelek és fájlok esetén.
- különböző biztonsági protokollok esetén, amikor hitelesíteni kell az ügyfeleket (pl.: LDAPS[9])

Az OpenSSL programcsomagot általában tanúsítványok elkészítéséhez használják sokszor azzal a céllal, hogy egy biztonságos kapcsolatot biztosító web oldal hitelességét és egyben biztonságát szavatolják. Ennek érdekében az elkészített tanúsítványt ajánlatos hitelesíteni, melynek menetét az ITU-T által kezelt X.509-es ajánlás tartalmazza. Amennyiben egy felhasználó olyan tanúsítvánnyal találkozik számítógépének használata közben, amit nem vizsgált be egy – CA (Certificate Authority)[10]– tanúsítványok hitelesítésével foglalkozó hatóság, akkor általában kap egy figyelmeztetést. Ilyen felugró, figyelmeztető ablakkal találkozhatunk például böngészés közben.

A tanúsítványokat tanúsító hatóságok (mint például a Symantec, GeoTrust) írják alá és ezzel érvényesítik az egyes cégek vagy egyének megbízhatóságát. Ennek költsége van, bár használatuk egyáltalán nem kötelező – azonban a felhasználók többsége számára megnyugvást jelenthet, hogy egy biztonságos web oldal meglátogatásakor figyelmeztetés megjelenése nélkül folytathatja a tevékenységét.

Nagy odafigyelést és felelősséget igényel a fejlesztő csapat munkája figyelembe véve, hogy hozzávetőlegesen a szerverek kétharmada ezt az ingyenes eszközkészletet használja. A magasan kvalifikált szakemberek eltökéltségén kívül némi pénzügyi forrásra is szükség van, ezért egy volt katonai tanácsadó[11] Maryland[12] államban létrehozta a „The OpenSSL Software Foundation, Inc." alapítványt az adományok, a tanácsadói szerződések[13] és az Egyesült Államok Belbiztonsági Minisztériumától és Védelmi Minisztériumától elnyert támogatások kezelésére.

[9] LDAP (Lightweight Directory Access Protocol) SSL felett.

[10] A tanúsító hatóság az a testület, amely a digitális tanúsítványok kiadásával foglalkozik.

[11] Az OpenSSL projekt fejlesztői csapatának önkéntes tagja.

[12] OpenSSL: http://en.wikipedia.org/wiki/OpenSSL (2014.05.05.)

[13] Steve Marquess: http://www.oss-institute.org/component/content/article/25-bios/57-steve-marquess (2014.05.05.)

2. KORÁBBI HIBÁK

Mielőtt elmélyülnénk a nemrégiben publikált súlyos OpenSSL hiba jellegzetességeiben érdemes megemlíteni néhány korábbi hibát érintőlegesen, amelyek hasonló sajátosságokat mutattak, mint a Heartbleed eset.

2008. május 13-án a Debian projekt bejelentett egy sebezhetőséget[14] az OpenSSL programcsomagban (kezdve a 0.9.8c-1 verziótól), mely hiba könnyen megjósolhatóvá, meghatározhatóvá tette a csomagban használt un. pszeudo-véletlenszám generátor kimeneti értékeit. Mindazonáltal az érintett debian alapú rendszereken készült SSH és/vagy SSL kulcsok véges halmazt alkottak, tehát nyers-erő módszerével véges időn belül visszafejthetővé váltak. Ennek ismeretében természetes, hogy a felhasználók számára teljesen észrevehetetlen maradhatott egy lehetséges man-in-the-middle támadás és a biztonságosnak hitt összeköttetésen átfolyó forgalmazás teljes visszafejtése is.

A probléma eszkalálódásához hozzájárult, hogy az elkészült kulcspárok bármilyen más rendszeren is felhasználásra kerülhettek, ezért a debian megoldásként javasolta a 2006. szeptember 17. és 2008. május 13. közötti időszakban[15], debian alapú rendszereken generált OpenVPN, DNSSEC, SSH (és a még sorolhatnánk) valamint SSL/TLS kulcsok esetében az összes tanúsítvány újragenerálását és a CA kulcsok visszavonását.

2012. április 24-én ismét publikálásra került OpenSSL hiba[16] a Debian projekt oldalán, mely valójában négy hiba együttes bejelentéséből tevődik össze:

- Az egyik közülük lehetőséget biztosít a támadónak MMA[17] támadásra, amivel meg lehet ismerni a felhasználó kulcsát.
- A másik bizonyos S/MIME[18] üzenetek elemzésekor szolgáltatás megtagadáshoz vezethet, amennyiben a támadó jól „megkomponált" üzenetet állított elő a sérülékeny rendszer számára.
- A leginkább érdekes mindközül az OpenSSL programcsomagban lévő DER[19] kódolt ASN.1[20] adat feldolgozásával foglalkozó függvény –

[14] *CVE-2008-0166*

[15] *DSA-1571-1 openssl -- predictable random number generator: https://www.debian.org/security/2008/dsa-1571 (2014.05.08.)*

[16] *CVE-2012-0884, CVE-2012-1165, CVE-2012-2110, CVE-2012-2131*

[17] *„Million Message Attack", melyet Daiel Bleichenbacher 1998-ban hozott nyilvánosságra tanulmányában.*

[18] *Secure/Multipurpose Internet Mail Extensions*

[19] *Distinguished Encoding Rules*

egész szám típusú adatra vonatkozó – értelmezési tévedése, melynek eredményeként a közismert „buffer overflow”[21] hibák egyik fajtáját a „heap[22] overflow”[23]-t lehet előidézni. A támadónak lehetősége nyílik olyan memória területre írni, amely túlnyúlik a neki biztosított határon – mindazonáltal tetszőleges kódot tud futtatni[24].

```
c.inf=ASN1_get_object(&(c.p),&(c.slen),&(c.tag),&(c.xclass),
                      len-off);

...
{
    /* suck in c.slen bytes of data */
    want=(int)c.slen;
    if (want > (len-off))
    {
        want-=(len-off);
        if (!BUF_MEM_grow(b,len+want))

        {
            ASN1err(ASN1_F_ASN1_D2I_BIO,
                    ERR_R_MALLOC_FAILURE);
            goto err;
        }
        i=BIO_read(in,&(b->data[len]),want);
```

2. ábra: Sebezhetőség az OpenSSl 0.9.6l-ben[25]

Az utóbb említett hiba külön érdekessége, hogy már 2006 novemberében publikálásra került Mark Dowd, John McDonald és Justin Schuhegy szerzők által a „The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities” című könyvben. Mark Down ugyan részletesen kifejtette a problémát, de akkor elfelejtette közölni olvasóival, hogy ez egy un. „0day”. (2. ábra)

---

[20] Abstract Syntax Notation One (ASN.1) szabványt az X.680-X.695 ITU ajánlás részletezi. Abstract Syntax Notation One (ASN.1) & ASN.1 encoding rules: http://www.itu.int/rec/T-REC-X.680-X.693-200811-I/en (2014.05.08.)

[21] Verem túlcsordulás

[22] Halom: A memóriának az a területe, amiből a blokkok dinamikusan foglalhatók le és szabadíthatók fel. A programok olyan adatokat tárolnak a halom memóriában, amelyekre a teljes futásidő egy részében van csak szükség.

[23] Halom túlcsordulás

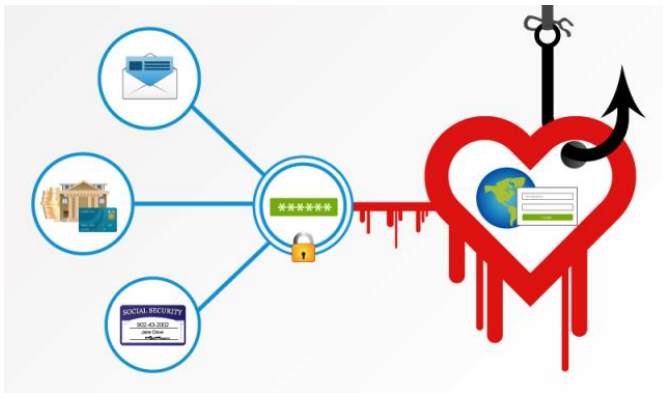
[24] DSA-2454-2 openssl -- multiple vulnerabilities: https://www.debian.org/security/2012/dsa-2454 (2014.05.08.)

[25] Mark Dowd, John McDonald, Justin Schuh: The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities Listing 6-6 Pearson Education, 2006 nov. 20 - 1200 oldal

3. A HEARTBLEED PROBLÉMA

A közelmúltban – az Interneten fellelhető – szinte minden sajtó a nettörténelem eddigi legnagyobb biztonsági résének felfedezéséről beszélt, amikor az OpenSSL.org által 2014. április 7-én bejelentett, CVE-2014-0160[26] néven „anyakönyvezett" sérülékenységről fejtették ki álláspontjukat. Könnyen elfogadható, hogy ez az aggodalom miért pont a világháló felhasználóit érinti leginkább – hiszen egyre inkább áttevődik a kommunikáció és az üzleti tevékenység erre a közegre.

A „Heartbleed bug" vagy gyakran „Heartbeat" néven emlegetett sérülékenység a közkedvelt OpenSSL titkosítási programcsomagot érinti, melyet rendszergazdák, hálózatadminisztrátorok, üzemeltetők és magánszemélyek egyaránt használnak a mindennapokban.



3. ábra: Heartbleed kapcsán leginkább érintett szolgáltatások[27]

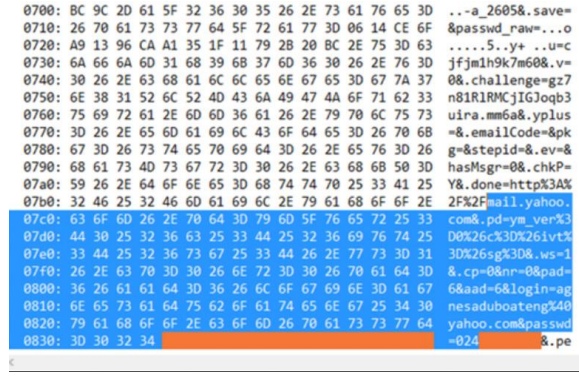
A csomagban feltárt hiba lehetőséget biztosít a támadónak, hogy hozzá tudjon férni olyan információkhoz, amiket alapesetben az SSL/TLS titkosított csatorna védene. Ez a csatorna a kommunikáció és az adatok – beleértve a jelszavak – biztonságát garantálja bizonyos web szerverek irányába, számos ügyfél hitelesítési megoldásban, pénzügyi tranzakciókban, a levelezésben, az üzenetküldőkben és a manapság egyre népszerűbb virtuális magánhálózatokban (VPN). (3. ábra)

[26] *OpenSSL Security Advisory [07 Apr 2014]: https://www.openssl.org/news/secadv_20140407.txt (2014.05.12.)*

[27] *http://www.zoho.com/vault/blog/the-heartbleed-bug-and-password-reuse-recipe-for-disaster.html (2014.05.09.)*

A bejelentett hiba bármely operációs rendszerrel rendelkező kliens és – a későbbiekben felsorolt – szerver kommunikációval van összefüggésben, aminek a lényege, hogy a kliens oldalról küldött felhasználói adat (payload) hossza soha nincs ellenőrizve. Ebből adódóan akár egy byte üzenet – szerver felé való – elküldése esetén is nyugodtan lehet állítani, hogy az 65535 (ez lehet a maximum érték a konkrét hibából adódóan) byte hosszú, aminek eredményeként 65535 byte adathoz jutunk hozzá a szerver memóriájából.

Az egyik legfontosabb kérdés az volt, hogy mekkora a valószínűsége annak, hogy az adatok között ott lesz a felhasználó privát kulcsa. A kérdésre gyorsan megjött a választ, több portálon publikálva, miszerint – ugyan elég „zajosan", sok próbálkozás után sikerül az adatokat kinyerni, viszont – a kulcsok megtalálhatók a kapott információk között. (4. ábra)



4. ábra: Szerver memóriájából kinyert adatok[28]

A nemrégiben napvilágra került Heartbleed sebezhetőség egy 2012. februárban megjelent RFC6520[29] szabvány hibás implementációjának hatására keletkezett. A szabvány[30] egy új, „TLS Heartbeat Extension" kiegészítést javasolt, mellyel az SSL kapcsolat minőségét lehet javítani. A szabvány által meghatározott TLS

[28] *Heartbleed OpenSSL (SSL/TLS) vulnerability – analysis of a mind-blowingly simple bug: http://geekslop.com/2014/heartbleed-openssl-ssl-tls-vulnerability-hacker-bug-analysis (2014.05.12.)*

[29] *Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) Heartbeat Extension, RFC6520.pdf: http://tools.ietf.org/pdf/rfc6520/ (2014.05.12.)*

[30] *Heartbleed – How Did Internet Security Almost Bleed Out?: http://www.symantec.com/connect/blogs/heartbleed-how-did-internet-security-almost-bleed-out (2014.05.12.)*

heartbeat úgy működik, mint egy „keep alive” (életben tartó) adatcsomag, aminek használatával az SSL kapcsolat egyik végén lévő számítógép duplán le tudja ellenőrizni azt, hogy a másik végén van-e még valaki. Ez a kiegészítés hasznos, mivel meg lehet akadályozni azt, hogy néhány régebbi router[31] – működéséből adódóan – megszakítsa az összeköttetést, ha azon nem áramlik adat.

Érintettség

A sebezhetőséget az OpenSSL 1.0.1 verziótól az 1.0.1f verzióig minden köztes kiadása tartalmazta, továbbá az OpenSSL:1.0.2:beta1 verziója. Az érintett, szerverként használt Linux disztribúciók közül néhány[32]:

- 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. május 10.) and 5.4 (OpenSSL 1.0.1c 2012. május 10.)
- FreeBSD 10.0 - OpenSSL 1.0.1e 2013. február 11.
- NetBSD 5.0.2 (OpenSSL 1.0.1e)
- OpenSUSE 12.2 (OpenSSL 1.0.1c)

A hiba kapcsán érintett – legismertebb – szolgáltatókat érdemes felsorolni a teljesség igénye nélkül, ahol tanúsítványokat és jelszavakat kell módosítani. (5. ábra)

Amazon Web Services (website üzemeltetőinek)	Google	SpiderOak
American Funds	Healthcare .gov	Tumblr
Box	IFTTT	USAA
Dashlane	Instagram	Venmo
Dropbox	LastPass	Wikipedia (ha van hozzáférési azonosító)
Etsy	Minecraft	Wordpress
Facebook	Netflix	Wunderlist
Flickr	OKCupid	Yahoo
GitHub	Pinterest	Yahoo Mail
Gmail	SoundCloud	YouTube
GoDaddy		

5. ábra a hiba kapcsán közvetlenül érintett szolgáltatók[33]

[31] *számítógép hálózatokban alkalmazott útválasztó eszköz*
[32] *The Heartbleed Bug: http://heartbleed.com/ (2014.05.12.)*

Az OpenSSL kapcsán feltárt hiba azért is gerjeszt sok tennivalót a javítások terén, mert a sebezhető kód nem csak kizárólag a web, email és kereskedelmi szervereket, a közösségi hálózatokat, a pénzügyi szektort, a kormányzati és adó portálokat sújtja. Az OpenSSL egyebek mellett hálózati eszközökben is felhasználásra került, ezért a gyártók közölték web oldalukon az érintett termékeik listáját. A Cisco közölte a potenciálisan sebezhető termékeinek listáját, melyből csak néhányat emelek ki, mivel a lista[34] több, mint 70 elemet tartalmaz:

- Cisco AnyConnect Secure Mobility Client for iOS [CSCuo17488]
- Cisco Cisco Internet Streamer CDS [CSCuo31566]
- Cisco Mobility Service Engine (MSE) [CSCuo20622]
- Cisco MS200X Ethernet Access Switch [CSCuo18736]
- Cisco ONS 15454 Series Multiservice Provisioning Platforms [CSCuo22921]
- Cisco Prime Security Manager [CSCuo27123]
- Cisco Security Manager [CSCuo19265]
- Cisco TelePresence IP Gateway Series [CSCuo21597]
- Cisco TelePresence Server 8710, 7010 [CSCuo21468]
- Cisco TelePresence Video Communication Server (VCS) [CSCuo16472]
- Cisco Unified 7800 Series IP Phones [CSCuo16987]
- Cisco Unified Communications Manager (UCM) 10.0 [CSCuo17440]
- Cisco Video Surveillance 3000 Series IP Cameras [CSCuo37282]
- Cisco WebEx Meetings Server versions 2.x [CSCuo17528]

Ugyanebben az üzleti szegmensben lévő másik gyártó, a Juniper is megtette ugyanezt – neki több mint 30 gyártmánya került publikálásra[35].

---

[33] The Heartbleed Hit List: The Passwords You Need to Change Right Now: http://mashable.com/2014/04/09/heartbleed-bug-websites-affected/ (2014.05.15.)

[34] OpenSSL Heartbeat Extension Vulnerability in Multiple Cisco Products: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140409-heartbleed (2014.05.12.)

[35] 2014-04 Out of Cycle Security Bulletin: Multiple products affected by OpenSSL "Heartbleed" issue (CVE-2014-0160): http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10623 (2014.05.12.)

4. Ajánlott javítások

A bejelentést követően a javítás kiadásáig elegendő idő állt rendelkezésre ahhoz, hogy a közismert szolgáltatóktól jelszavak, privát kulcsok szivároghattak ki, mivel az előzőekben említett adatkinyerést is egy napon belül publikálták.

Kinek, mit kell tennie annak érdekében, hogy a biztonságérzetet visszahozzuk a korábbi szintre? A *fejlesztők* ugyan kiadták a javítást (OpenSSL 1.0.1g) a leginkább használt architektúrákra, azonban a többiről is gondoskodni kell.

A *rendszergazdáknak* a szükséges javításokat minél hamarabb a szerverekre kell telepíteni és a tanúsítványokat le kell cserélni. A korábban belépett és még kapcsolatban lévő felhasználókat ki kell léptetni az újra belépéshez. Még mai is rengeteg olyan szerver van, amelyiken nem történt meg a frissítés, mert:

- ugyan elérhető és letölthető a korrigált kód az adott rendszerre, azonban kevesen javítanak azonnal.
- még nem áll rendelkezésre a javított kód installálható állapotban, csak forrásból lehetne az adott rendszerre fordítani, mely komolyabb kihívást jelent. A cikk írásának pillanatában ilyen pl.: Debian Wheezy (stable) armel architektúrára.

A *felhasználóknak* meg kell vizsgálni, hogy mely szolgáltatásokon tároltak érzékeny, személyes adatokat, leveleket, és melyeken intézték pénzügyeiket, biztosításukat. Legelőször itt szükséges jelszavakat módosítani, miután a rendszer javítása már megtörtént.

A cikk bemutatott néhány korábban feltárt sebezhetőséget is az OpenSSL programcsomagban, melyek aggodalommal töltik el a felhasználókat. A bizalom egyértelműen megrendült. Mindezt alátámassza az is, hogy az OpenBSD csapat az eredeti OpenSSL forrásból kiindulva új projektet indított el LibreSSL[36] néven a botrány kirobbanás után nem sokkal, 2014. április 22-én. A projektnek az a célja, hogy ingyenes, SSL/TLS protokollt támogató eszközkészletet biztosítsanak, remélve, hogy kevesebb sérülékenység keletkezik a kódban. Az első héten több mint 90000[37] – C programnyelven megírt – sort vettek ki a korábbi forráskódból.

5. Nemzetbiztonsági szempontok

Az OpenSSL könyvtár 2012. eleje óta tartalmazta a sérülékenységet, amelyen keresztül támadók észrevétlenül hozzáférhettek az OpenSSL programcsomagot

[36] *LibreSSL: http://www.libressl.org (2014.05.12.)*
[37] *LibreSSL: http://en.wikipedia.org/wiki/LibreSSL (2014.05.12.)*

használó eszközök memóriájához és onnan közvetlenül képesek voltak adatokat és privát kulcsokat eltulajdonítani. Amennyiben valakinek birtokába kerülnek ezek az információk, akkor a titkosított információk könnyen visszafejthetők.

Figyelembe véve a Snowden[38] által nyilvánosságra hozott – vélhetően működő – NSA adatgyűjtési módszereket kézenfekvő, hogy az internet felhasználókban felmerül a gyanú, hogy ez a hiba nem véletlenül van a forráskódban. Ennek ügyes felhasználói lehettek a nemzetbiztonsági szolgálatok.

A Bloomberg[39] azt fejti ki cikkében, hogy a National Security Agency (NSA) legkevesebb két éve tudott a Heartbleed sérülékenységről, de azt titokban tartotta. Felhasználta információk gyűjtésére például más országok számítógépes rendszereiről, potenciális terrorista szervezetekről, nukleáris csempészekről és kormányokról. Természetesen az NSA tagadja, hogy tudott a Heartbleed-ről és ezt azzal támassza alá, hogy a Szövetségi kormány is az OpenSSL-t használva védi a kormányzati intézmények weboldalait és más online szolgáltatások felhasználóit. A National Security Agency több ezer informatikai biztonsági szakértőt foglalkoztat azzal a céllal, hogy szoftverekben, de leginkább nyílt forrásúakban sérülékenységet keressenek[40]. A sérülékenység felhasználásával olyan eszközök hozhatók létre, melyekkel könnyedén lehet ezután belépési azonosítókat, jelszavakat gyűjteni a közösségi hálózatoktól kezdve a levelező szerverekig.

A jelszavak alapján könnyen meg lehet határozni egy adott személy jelszó képzési algoritmusát, ami nagy segítséget nyújt a jelszavak visszafejtésében olyan rendszerek esetén, ahol nincs sérülékenység az információszerzés kivitelezéséhez.

Bármely ország nemzetbiztonsági szolgálata vagy rendvédelmi szerve adott ügy kapcsán fel van hatalmazva, hogy – bizonyos feltételek teljesülése esetén – információkat gyűjtsön. Amennyiben „egy ajtó nyitva áll előtte”, akkor azt az ügy érdekében ki fogja használni. Mindenki számára ismert, hogy 0day sérülékenységek értékesítési piaca elég nagy forgalmat bonyolít. A vevők között ugyanúgy ott

[38] Edward Snowden: Amerikai számítógépes szakember, amerikai Nemzetbiztonsági Ügynökség (NSA) és a Központi Hírszerző Ügynökség (CIA) volt alkalmazottja.

[39] Bloomberg News: egy nemzetközi hírügynökség.

[40] NSA Said to Exploit Heartbleed Bug for Intelligence for Years: http://www.bloomberg.com/news/2014-04-11/nsa-said-to-have-used-heartbleed-bug-exposing-consumers.html (2014.05.12.)

vannak a szolgálatok is. Leghatékonyabbak azok a sebezhetőségek tudnak lenni, amit más még nem ismer[41].

Ma már mindenki számára elérhető és letölthető a Heartleech eszköz, mellyel ki lehet aknázni a Heartbleed sérülékenységben rejlő lehetőségeket[42].

Összegzés

Jelen cikkben kifejtésre került néhány OpenSSL programcsomagot érintő hiba a korábbi évekből és a mostani, nagy sajtóvisszhangot megért Hearttbleed sérülékenység. Mindegyikben vannak közös vonások és eltérések.

Az eltérés leginkább a konkrét hiba okában és némileg a realizálódásban lelhető fel. Azonban figyelemre méltó, hogy az egyik esetben a hiba a disztribútor – vagyis a Debian team – részéről került bele a kódba. Az OpenSSL projekt vétlen volt. Itt a programozói hibát egy adminisztratív hiba is követte, aminek eredményeként a kódot módosító személy közvetlenül, kvázi ellenőrzés nélkül tudta érvényre juttatni hibás sorait.

Azonosságból több tapasztalható, melyek közül felsorolnám a lényegeseket:

- Érdekessége mindegyik hibának, hogy jóval a valós keletkezése után került be a köztudatba. Az egyik esetben ez a megjelent könyv félreértéséből vagy meg nem értéséből adódhatott, azonban a többi esetben ez inkább a nyílt forráskóddal szemben mutatott bizalmat jelenti. Annyira nagy a bizalom a nyílt forráskódú programok használatával kapcsolatban, hogy senki nem nézi meg magát a forrást a hétköznapi felhasználók közül. Mindenki abban bízik, hogy már más megvizsgálta vagy kielemezte a szoftvert és amennyiben az ideje engedi akkor a felhasználó maga is bármikor megnézheti.
- Tovább fokozta a hibák súlyát, hogy man-in-the-middle támadást lehetett velük végrehajtani, ezáltal személyes adatokat, jelszavakat és tanúsítványokat lehetett eltulajdonítani.
- A végén mindegyik hiba nyilvánosságra került, ami a nyílt forráskódnak köszönhető. Még nagyobb port kavartak volna az esetek, ha bármelyik hibajavítás a háttérben zajlik. Ez dobozos szoftverek esetén elég gyakori.

---

41 NSA purchased zero-day exploits from French security firm Vupen: http://www.zdnet.com/nsa-purchased-zero-day-exploits-from-french-security-firm-vupen-7000020825/ (2014.05.12.)

42 heartleech: https://github.com/robertdavidgraham/heartleech: (2014.05.12.)

A nemzetközi (leginkább a nyugati) sajtó sérülékenységgel kapcsolatos elemzéseit olvasva az tapasztalható, hogy az utóbbi időben – főleg a Stuxnet[43] és a Snowden ügy után – egyre jobban elterjed a köztudatban az a vélemény, hogy minden szoftver hiba mögött nagy nemzetek nemzetbiztonsági szolgálatai állnak.

Felül kell vizsgálni a nyílt forráskódú rendszerekbe vetett korábbi bizalmat az új kormányzati rendszerek kiválasztásánál, ill. régebbiek kiváltásánál. Amennyiben lehetséges alternatívaként továbbra is szerepet kap, akkor ki kell használni azt a lehetőséget, hogy a forráskódot ki lehet elemezni, le lehet tesztelni és tovább lehet fejleszteni saját célokra.

Radikális fordulatot kell végrehajtani a fejlesztések és kivitelezések végrehajtása terén annak érdekében, hogy a biztonsági kérdésekre ellenőrzésére elég idő maradjon olyan kormányzati területeken, ahol az információ kiszivárgásának megakadályozása elsődleges szempont.

Felhasznált források:

1. Project Newsflash!: https://www.openssl.org/news/ (2014.05.05.)
2. Welcome to the OpenSSL Project: https://www.openssl.org/ (2014.05.05.)
3. OpenSSL: http://en.wikipedia.org/wiki/OpenSSL (2014.05.05.)
4. Steve Marquess: http://www.oss-institute.org/component/content/article/25-bios/57-steve-marquess (2014.05.05.)
5. Certificate Lifecycle: http://wiki.openssl.org/index.php/Certificate_Lifecycle (2014.05.05.)
6. DSA-1571-1 openssl -- predictable random number generator: https://www.debian.org/security/2008/dsa-1571 (2014.05.08.)
7. DSA-2454-2 openssl -- multiple vulnerabilities: https://www.debian.org/security/2012/dsa-2454 (2014.05.08.)
8. Abstract Syntax Notation One (ASN.1) & ASN.1 encoding rules: http://www.itu.int/rec/T-REC-X.680-X.693-200811-I/en (2014.05.08.)

[43] *Feltételezések szerint az USA/Izraelben által fejlesztett kártevő, mely az iráni urándúsító centrifugák működését kívánta megzavarni.*

9. Mark Dowd, John McDonald, Justin Schuh: The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities Listing 6-6 Pearson Education, 2006 nov. 20 - 1200 oldal
10. http://www.zoho.com/vault/blog/the-heartbleed-bug-and-password-reuse-recipe-for-disaster.html (2014.05.09.)
11. The Heartbleed Hit List: The Passwords You Need to Change Right Now: http://mashable.com/2014/04/09/heartbleed-bug-websites-affected/ (2014.05.15.)
12. OpenSSL Security Advisory [07 Apr 2014]: https://www.openssl.org/news/secadv_20140407.txt (2014.05.12.)
13. The Heartbleed Bug: http://heartbleed.com/ (2014.05.12.)
14. heartleech: https://github.com/robertdavidgraham/heartleech: (2014.05.12.)
15. OpenSSL Heartbeat Extension Vulnerability in Multiple Cisco Products: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140409-heartbleed (2014.05.12.)
16. 2014-04 Out of Cycle Security Bulletin: Multiple products affected by OpenSSL "Heartbleed" issue (CVE-2014-0160): http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10623 (2014.05.12.)
17. Heartbleed – How Did Internet Security Almost Bleed Out?: http://www.symantec.com/connect/blogs/heartbleed-how-did-internet-security-almost-bleed-out (2014.05.12.)
18. Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) Heartbeat Extension, RFC6520.pdf: http://tools.ietf.org/pdf/rfc6520/ (2014.05.12.)
19. Heartbleed OpenSSL (SSL/TLS) vulnerability – analysis of a mind-blowingly simple bug: http://geekslop.com/2014/heartbleed-openssl-ssl-tls-vulnerability-hacker-bug-analysis (2014.05.12.)
20. LibreSSL: http://www.libressl.org (2014.05.12.)
21. LibreSSL: http://en.wikipedia.org/wiki/LibreSSL (2014.05.12.)
22. NSA Said to Exploit Heartbleed Bug for Intelligence for Years: http://www.bloomberg.com/news/2014-04-11/nsa-said-to-have-used-heartbleed-bug-exposing-consumers.html (2014.05.12.)
23. NSA purchased zero-day exploits from French security firm Vupen: http://www.zdnet.com/nsa-purchased-zero-day-exploits-from-french-security-firm-vupen-7000020825/ (2014.05.12.)