HEARTBLEED БЪГ: ЗАПЛАХА ЗА ИНТЕРНЕТ СИГУРНОСТТА И МЕТОДИ ЗА ЗАЩИТА*

КРАСИМИР М. КОРДОВ

HEARTBLEED BUG: THREAT FOR INTERNET SECURITY AND METHODS FOR PROTECTION

KRASIMIR M. KORDOV

ABSTRACT: *One of the biggest vulnerability of internet was detected several months ago. The security breach is found in OpenSSL (performing the secure internet connection) used by 2/3 of all servers of the world. The Heartbleed Bug affected millions of websites and allowed hackers to steal sensitive information such as usernames and passwords of tens of millions people around the world. In this paper Heartbleed Bug is explained and methods for protection are proposed.*

KEYWORDS: *Heartbleed Bug, OpenSSL vulnerability, Internet security*

Въведение: Предаването на важна информация като потребителски имена и пароли в глобалната мрежа е основна цел на компютърната и мрежова сигурност [1, 2]. Защитата на предаваните данни по мрежата се осъществява чрез криптиращи протоколи интегрирани както на сървърите, така и на потребителските компютърни устройства. Едно от най-често използваните решения за сигурност при предаване на данни в интернет е OpenSSL - програмна библиотека написана на C++ [3, 4]. Фактът че тази библиотека е с отворен код и е използвана от две трети от сървърите по целия свят, предизвиква голям интерес и е обект на непрестанни атаки от хакерите и хакерските групировки. OpenSSL предоставя необходимата сигурност и въпреки многобройните атаки е един от най-добрите методи за криптирано предаване на данни, който се усъвършенства с всяка нова версия.

Неочаквано в началото на месец Април 2014 беше съобщено за уязвимост в OpenSSL, позволяваща източването на голямо количество потребителски имена, пароли и криптографски ключове от паметта на сървърите по цял сят. Широкото използване на тази библиотека от милиони сървъри, на които са разположени голяма част от всички сайтове, е позволило на хакерски групировки да се сдобият с данните на потребители от всички държави. Засегнати са сървъри на едни от най големите компании като Adobe, Yahoo, Sony и др. [5]. При евентуална атака на конкретен сървър (било то и на световно известна компания) щетите биха били сравнително по-малки, но откритият бъг засяга сигурността на интернет в глобален мащаб.

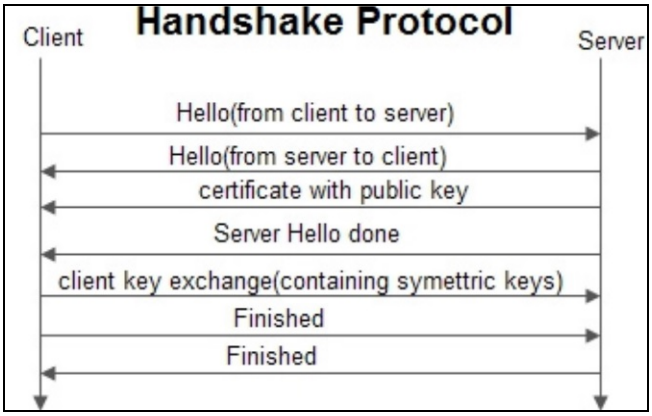
Функционалност на OpenSSL: OpenSSL [6] е реализация (с отворен код) на протоколите Transport Layer Security(TLS) и Secure Sockets Layer (SSL). Тези протоколи съдържат криптографски алгоритми за осъществяване на сигурно предаване на данни в интернет. Криптираната комуникация се използва от повечето сайтове и приложения които дават достъп до интернет банкиране, изпращане на имейли, съобщения и др.

SSL/TLS предоставя три важни функции [7]:

* Настоящата статия е финансирана от Фонд „Научни изследвания” към Шуменския университет „Епископ Константин Преславски“ по проект № РД-08-236/13.03.2014 г.

1. Удостоверяване – осъществява се чрез цифрови сертификати и RSA криптографски алгоритми [8]. Проверява се за наличните сертификати и се избира най-сигурния от тях, за осъществяване на криптирана връзка.
2. Конфиденциалност - обменяната информация между участниците в комуникацията, може да се декриприта само от удостоверените участници разполагащи със симетричният ключ, разменен при стъпка 1.
3. Цялост на съобщенията – съобщенията, обменяни между участниците в комуникацията , не трябва да бъдат променяни чрез външни намеси. С цел да се запази целостта на съобщенията се използват функции за хеширане като MD5 и SHA1.

Започването на криптирана връзка между клиент и сървър се извършва от процедура наречена „ръкостискане“.



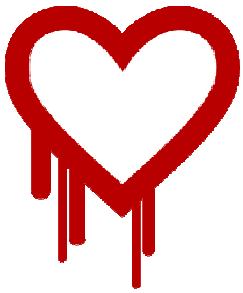
Фигура 1

На фигура 1 е показана поредността на стъпките необходими за стартирането на връзка клиент-сървър. Най-важните елементи на тази процедура е „уточняването“ на сертификата който ще се използва за криптирана връзка и обмяната на симетричните криптографски ключове.

Heartbleed бъг: След разгледаният модел на работа на OpenSSL, който реализира протоколите SSL и TLS не се забелязват пропуски в методиката и принципите на работа при осъществяването на сигурна комуникация в интернет. Откритият пропуск е свързан с техническа реализация на една от допълнителните услуги в програмният код на OpenSSL. С цел пестене на ресурси е реализирана услуга наречена “keep alive”, която поддържа „жива“ отворената връзка, като обменя съобщения с много кратко случайно съдържание между клиента и сървъра. Случайното съобщение е в размер на 1 байт информация, която е случаен фрагмент от паметта на компютърното устройство на клиента или на сървъра. Този незначителен, малък обем на информация не представлява опасност и услугата “keep alive” напълно реализира целта си. Проблемът идва от самата реализация която индексира началото на съобщението чрез указател към паметта и възможността на клиента да променя програмния код, тъй като OpenSSL е с отворен код. **Чрез промяна на големината на исканото съобщение от сървъра може да се извлича информация от паметта на сървъра с размер до 2 килобайта.** [9, 10] По този начин е въпрос на време да се източи информацията записана в паметта на сървъра. Естеството на самата информация прави уязвима цялата глобална мрежа, тъй като на сървърите основните записани данни са потребителските имена, паролите и лични данни на потребителите, както и криптографските ключове, използвани от сървърите.

За съществуването на този пропуск в сигурността, засягащ 2/3 от сървърите по цял свят, е съобщено на 1.04.2014г. Програмистът от Google - Neel Mehta и екипът на

финландската фирма Codenomicon, занимаваща се с компютърна сигурност, направили съобщенията си, като открили проблема независимо един от друг. [11] Инженер от Codenomicon е дал името на откритият бъг “Heartbleed Bug” отчитайки първоначалното име на услугата “keep-alive” – “Heartbeet”. Финландската фирма разработва сайт [12] на който кратко е обяснено какво представлява Heartbleed и представя официалното лого на този бъг (фигура 2).



Фигура 2

След анонсирането на Heartbleed, всички световни медии отразиха новината като една от най големите заплахи в историята на съществуването на интернет. Големият брой сървъри предоставящи услуги, чрез криптирана връзка, използващи OpenSSL са били изложени на потенциално източване на данните на потребителите си. Взети са незабавни мерки и още във следващата излязла версия на OpneSSL проблемът е отстранен, но никой не може да каже със сигурност размерът на щетите на засегнатите от огромното изтичане на информация от сървъри по целия свят. Предполага се съществуват фирми, които са били наясно с тази уязвимост, тъй като са използвали променени версии на OpenSSL и не са засегнати от Heartbleed. Тревожен е и фактът че, според анонимни източници, работещи в Американската Агенция за Сигурност (NSA), агенцията от 2-3 години е знаела за проблема и не са го анонсирали, за да го използват за лични цели. [13]

Методи за защита: В новите версии на OpenSSL този бъг е отстранен. Методите за защита са свързани с ограничаване от последиците и превенциите от изтичането на информация в глобален мащаб. Необходими са действия освен от програмистите, реализиращи OpenSSL, администраторите на сървърите, така и от потребителите използващи интернет по целия свят.

Разработчиците на OpenSSL – необходимо е всички основни управляващи функции на OpenSSL да бъдат съсредоточени изцяло (или доколкото е възможно) в сървърната част. По този начин ще се ограничи възможността на злонамерени потребители да манипулират данни и заявки изпращани в процеса на криптирана комуникация.

Администратори на сървъри – необходимо е незабавно обновяване на версията на OpenSSL. Все още съществува голям брой сървъри предоставящи услуги които използват OpenSSL и не са обновили своята версия. Собствениците на такива сървъри често правят еднократна инвестиция, като плащат за инсталиране на необходимият софтуер и не залагат необходимите разходи за поддръжка и обновяване на софтуера. Разходите са напълно оправдани и гарантират сигурността на данните на потребителите, съхранявани на сървъра. Необходимо е непрекъснат мониторинг на развитието на използваният софтуер и неговото обновяване.

Потребителите на интернет – въпреки отричането на големите компании, че има каквато и да е опасност за потребителите им, всеки трябва да приеме че е възможно паролите които използва да са „откраднати“. Всеки потребител използващ интернет банкиране, електронна поща и други услуги изискващи криптирана връзка, трябва периодично да сменя своите пароли. Необходимо е да се спазват познатите правила за дължина на използваните

пароли, включването на цифри, символи и горен и долен регистър на буквите в паролите. Heartbleed предизвика изработването на сайтове който показват коя версия на OpenSSL използват сървърите и дали са уязвими. Един от сайтовете на който може да се провери за уязвимост от този бъг е: https://filippo.io/Heartbleed/ . Потребителите на смартфони и таблети с операционна система Android трябва да знаят че тази операционна система също работи с OpenSSL и също трябва да проверяват своите устройства дали са засегнати. GooglePlay предоставя възможност на потребителите на най-широко използваните операционни системи Android, да изтеглят безплатно приложение - Heartbleed Security Scanner [14] чрез което да сканират своето устройство и да проверят своята версия на OpenSSL.

Заключение: Откритият пропуск в сигурността на интернет не бива да се подценява, защото засяга огромен брой сървъри по целия свят и изтичането на информация засяга милиони потребители. Въпреки старанието на големите компании, да не предизвикват паника у своите потребители, като не съобщават за щетите, е необходимо потребителите незабавно и регулярно да сменят своите пароли, защото по всяка вероятност паролите им вече са били компрометирани. Администраторите на сървърите трябва непрекъснато да следят за новите версии на протоколите за сигурност и периодично да обновяват софтуера на сървърите, за да защитят информацията на своите потребители.

ЛИТЕРАТУРА

1. **Станев, Ст.,** Ст. Железов. Компютърна и мрежова сигурност, ЦДО, Шумен, 2005
2. **Железов, С.,** А. Начев, Статистически модел за оценка на въздействието на заплахите за компютърните системи и мрежи, Научна конференция „Защита на личните данни в контекста на информационната сигурност", НВУ „Васил Левски", Шумен, 2013
3. **Йовчева Б.**, И. Иванова ПЪРВИ СТЪПКИ В ПРОГРАМИРАНЕТО НА C/C++, София, 2007
4. **Стоянов, Б**., Програмиране I, Модул 1, ЦДО Шумен, 2013
5. **URL:** http://hackingnews.com/vulnerability/heartbleed-hit-list-affected-websites/ (14.09.2014)
6. **URL:** http://en.wikipedia.org/wiki/OpenSSL (14.09.2014)
7. **Mpofu, T., N. Elisa, N Gati,** The Heartbleed Bug: An Open Secure Sockets Layer Vulnerability, IJSR, Volume 3 Issue 6, June 2014
8. **URL:** http://en.wikipedia.org/wiki/RSA (14.09.2014)
9. **URL:** www.cphpvb.net/network-security/9444-openssl-heartbleed-explained/ (14.09.2014)
10. **URL:** http://vrt-blog.snort.org/2014/04/heartbleed-memory-disclosure-upgrade.html (14.09.2014)
11. **URL:** http://en.wikipedia.org/wiki/Heartbleed (14.09.2014)
12. **URL:** http://heartbleed.com/ (14.09.2014)
13. **URL:** http://www.usatoday.com/story/tech/2014/04/11/heartbleed-cisco-juniper/7589759/ (14.09.2014)
14. **URL:** https://play.google.com/store/apps/details?id=com.lookout.heartbleeddetector (14.09.2014)