Heartbleed - The Vulnerability That Changed the Internet

Ionuț-Daniel BARBU, Ioan BACIVAROV
EUROQUALROM, University POLITEHNICA of Bucharest, Romania
barbu.ionutdaniel@gmail.com, bacivaro@euroqual.pub.ro

Abstract

This article is intended to present the Heartbleed bug and will include information from statistical aspects and impact of the vulnerability to an overview of how it actually works. In addition to this, a reproduction of the exploit is described and some affected software distributions listed. For educational purposes, during this research a vulnerable version of Apache server has been targeted. The well - known, low cost device RaspberryPI built on ARM architecture serves as the hardware platform for the targeted machine and it supports a Linux image. Heartbleed vulnerability has been categorized as a critical vulnerability of the cryptographic software library OpenSSL and its name has proven to be a good choice from various perspectives. 14th of March 2012 is the day when the bug has been released after its introduction in the code. Although the discovery's precise time is questionable by a lot of critics, at least the public disclosure date is known and that is 1st of April 2014. So 2 years have passed without notification of the existence of the bug and this raised some discussions. Some of them also targeted the SSL/TLS encryption itself as its original purpose was to protect the information. It seems that Heartbleed was introducing the exact opposite aspect of this by giving attackers the chance to gather valuable information from system's memory. By valuable we are referring to highly sensitive information including secret keys used for traffic encryption. From a statistical point of view it is worth mentioning that it affected two thirds of the Internet as the base servers were running OpenSSL. In terms of traces left by the attack exploiting it, unfortunately it is highly unlikely to discover abnormal activity in system's logs. The conclusion we reached while writing this article is that this vulnerability is extremely serious therefore it should be studied and tested against.

Index terms: Heartbleed, OpenSSL, RaspberryPI, vulnerability

References:

[1]. J. Erickson, Hacking: the Art of Exploitation, 2nd Edition, No Starch Press, 2008.

[2]. Z. Durumeric, F. Li, J. Kasten, J. Amann, J. Beekman, M. Payer, N. Weaver, A. David, V. Paxson, M. Bailey, and J. A. Halderman, The Matter of Heartbleed, ACM Internet Measurement Conference (IMC'14), 2014.

[3]. B. Chandra, A technical view of the OpenSSL 'Heartbleed' vulnerability, White paper, IBM developerWorks, May 2014.

[4]. Heartbleed, (2014, Jul 12) [Online]. Available: http://heartbleed.com/

[5]. Heartbleed, (2014, Jul 15) [Online]. Available: en.wikipedia.org/wiki/Heartbleed

[6]. CVE, (2014, Jul 21) [Online]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi ?name=CVE-2014-0160

[7]. OpenSSL, (2014, Aug 05) [Online]. Available: www.openssl.org/news/ secadv_20140407.txt

[8]. NMap, (2014, Aug 05) [Online]. Available: https://svn.nmap.org/nmap/scripts/ssl-heartbleed.nse