Proceedings of the 14th International Conference on Quality and Dependability
Sinaia, Romania, September 17th-19th, 2014
ISSN 1842-3566
Pages 100-109

The Heartbleed Bug – A Vulnerability in the OpenSSL Cryptographic Library

Ionuţ-Daniel BARBU, Ioan C. BACIVAROV
Dell SecureWorks; EUROQUALROM Laboratory, Faculty of Electronics, Telecommunications and Information Technology, University POLITEHNICA of Bucharest, Romania
barbu.ionutdaniel@gmail.com

Abstract
The purpose of this article is to present various aspects of the Heartbleed bug including a general overview of the vulnerability, details related to how it works, affected software distributions and statistical observations. Moreover, the paper presents the exploitation of a vulnerable version of an Apache server. The targeted machine is represented by a Linux image for ARM architecture installed on a RaspberryPI device. The Heartbleed Bug is a very intelligently chosen name for a serious vulnerability discovered in the OpenSSL Cryptographic software library. The vulnerability was erroneously introduced in the code and released on the 14th of March 2012. More than 2 years later, on April 1st it was discovered and publically disclosed. The SSL/TLS encryption, by design and implementation it's meant to protect the information. The consequence of this vulnerability is allowing attackers to obtain and read the memory of the systems and may lead to leaking information such as very sensitive information related to secret keys used to identify the service providers and to encrypt the traffic. Statistically speaking two thirds of the internet's web servers use OpenSSL. It is worth mentioning that exploitation of this bug does not leave any trace of anything abnormal happening to the logs. Studying this vulnerability and performing tests in the informational environment is critical and we highly recommend it.

References:

[1] HACKING: THE ART OF EXPLOITATION, 2ND EDITION, Jon Erickson, No Starch Press 2008
[2] http://heartbleed.com/
[3] http://en.wikipedia.org/wiki/Heartbleed
[4] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
[5] https://www.openssl.org/news/secadv_20140407.txt
[6] https://www.schneier.com/blog/
[7] http://www.theguardian.com/technology/
[8] http://www.bbc.com/news/technology-27155946
[9] http://gizmodo.com/
[10] http://tools.cisco.com
[11] http://en.wikipedia.org/wiki/Raspberry_Pi
[12] http://en.wikipedia.org/wiki/Openssl
[13] http://www.kali.org/
[14] https://svn.nmap.org/nmap/scripts/ssl-heartbleed.nse
[15] https://svn.nmap.org/nmap/nselib/tls.lua