

**ECE 9069:** *CVE-2014-0160 Heartbleed*

Group:

Wei Dai,

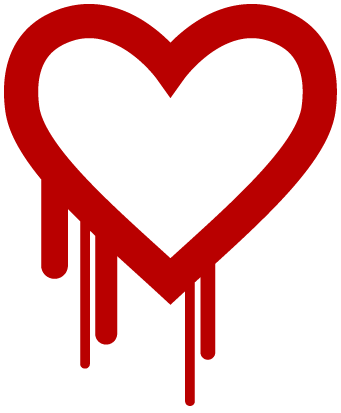
Yongxun YU,

Xiling Wang

Department of Electrical & Computer Engineering

The University of Western Ontario

**Terms Used in the Report**



1. CVE

CVE stands for common vulnerabilities and exposures.

It is a publicly disclosed database that contains information security issues. CVE was launched by MITRE Corporation firstly in 1999. It is now managed and maintained by the National Cybersecurity FFRDC (Federally Funded Research and Development Center). Additionally, the sponsor of CVE is US Federal Government, with both the US Department of Homeland Security (DHS) and the Cybersecurity and Infrastructure Security Agency (CISA) [^1]

CVE is similar to a free dictionary for individuals and organizations to improve their information level by identifying, defining, and cataloging publicly disclosed cybersecurity vulnerabilities. [^2]

1. Vulnerability

A vulnerability, a kind of flaw in software code, could be used by hackers to gain direct access to a system or network. Normally, hackers could act as super-power administrators by taking advantage of vulnerabilities in a system. Plus, both access and actions are mostly unauthorized. [^3]

1. OpenSSL

OpenSSL software is a robust, commercial-grade, full-featured toolkit for general-purpose cryptography and secure communication developed by OpenSSL Project. [^4]

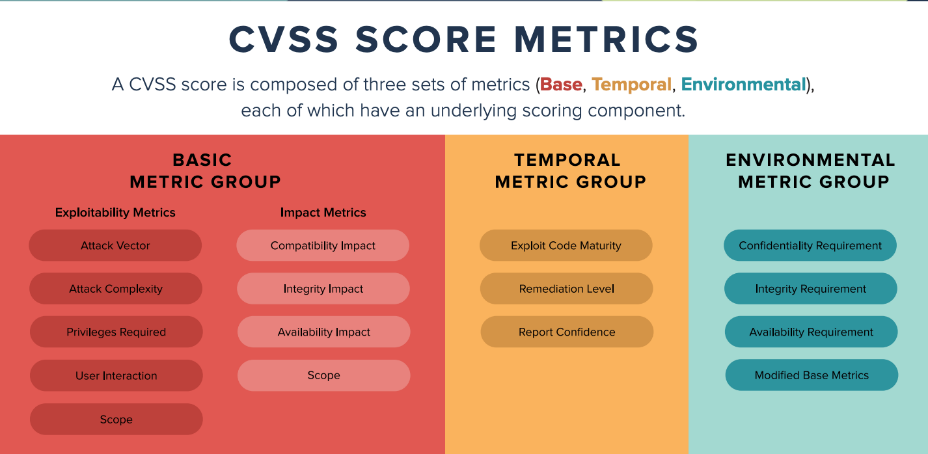
1. SSL/TLS

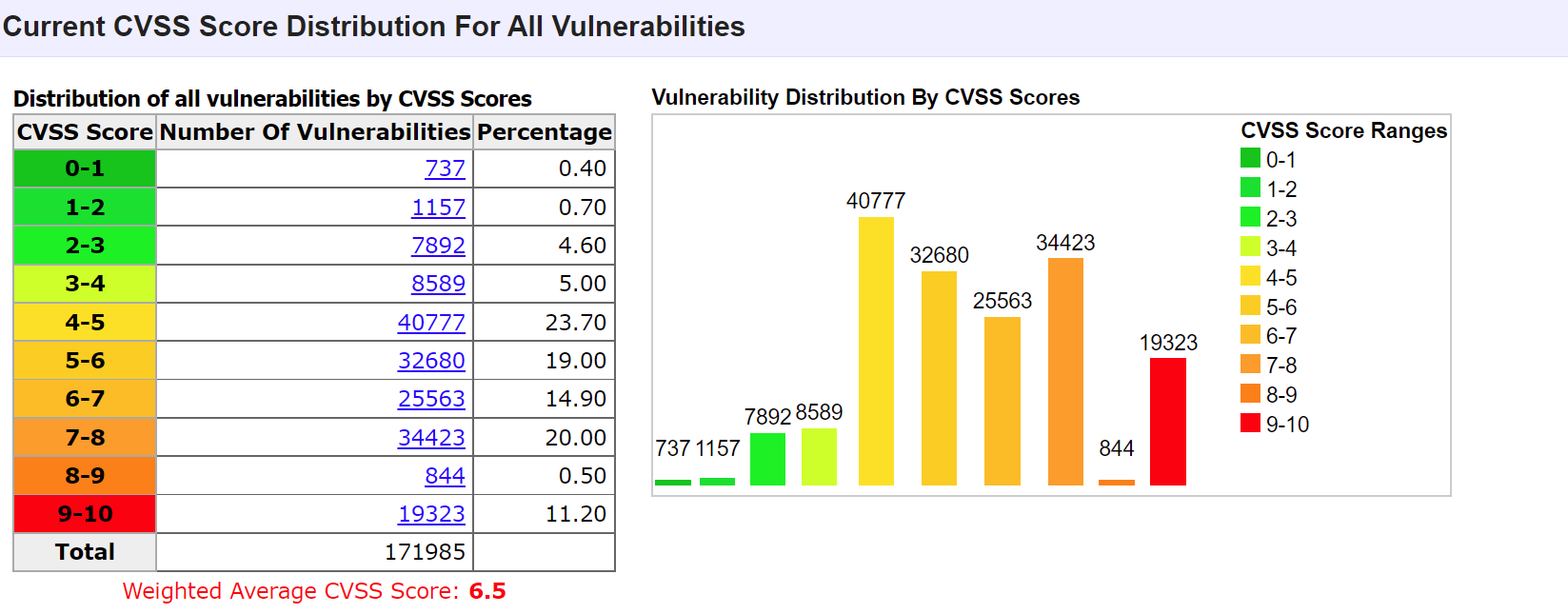
SSL/TLS provides communication security and privacy over the Internet for applications such as web, email, instant messaging (IM), and some virtual private networks (VPNs). The Heartbleed bug is not a design flaw in SSL/TLS protocol specification. It is an implementation issue when the OpenSSL library provides SSL/TLS cryptographic services to the application. [^5]

1. CVSS

CVSS stands for Common Vulnerability Scoring System. This system provides a numerical (0-10) representation of the severity of an information security vulnerability. The more serious the vulnerability is the higher score.

|  |  |
| --- | --- |
| CVSS Score | Qualitative Rating |
| 0.0 | None |
| 0.1 – 3.9 | Low |
| 4.0 – 6.9 | Medium |
| 7.0 – 8.9 | High |
| 9.0 – 10.0 | Critical |

[^6]

[^7]

**CVE-2014-0610**

1. Description

Every specific vulnerability in CVE corresponds to a serial number. CVE-2014-0160 refers to the Heartbleed bug. “*The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet.”* [^5]

It allows anyone to read the memory of the protected system with the version of the vulnerable OpenSSL software. Attacks have the accessibilities to eavesdrop on communications, steal data directly from the services and users, and impersonate services and users.

Although this bug could be fixed by the new version released, it has already exposed a large number of encryption and decryption keys to the public. Therefore, the Heartbleed bug is considered a seriously treated and unique vulnerability because of the long exposure and ease of no trace attacks.

1. Origin of Heartbleed

Heartbleed is an extension of the OpenSSL’s implementation of the TLS/DTLS heartbeat (RFC6520). When this is exploited, the memory leakage occurs from both the direction of the server to the client and the client to the server.

1. CVSS Scores & Vulnerability Types

|  |  |
| --- | --- |
| CVSS Score | **5.0** |
| Confidentiality Impact | Partial (There is considerable informational disclosure.) |
| Integrity Impact | None |
| Availability Impact | None |
| Access Complexity | Low (Little knowledge or skill is required to exploit. ) |
| Authentication | Not required |
| Gained Access | None |
| Vulnerability Type(s) | Overflow Obtain Information |
| CWE ID | [119](https://www.cvedetails.com/cwe-details/119/cwe.html) |

[^8]

1. Overflow and Obtain information

Chart, bar chart

Description automatically generated[^9]

According to the Statistical data from CVE details website, overflow is the most common type of vulnerability with publishing dates after 1999. Overflow occurs when there is more data needs to be stored in a fixed size of memory. The extra information may overflow into adjacent memory space and usually cause system crashes and memory leakage.

Obtain Information, also known as information disclosure vulnerability, is leaking sensitive data unintentionally to its user or the public. Depending on the different context of different websites, all kinds of information including:

* Users’ data, such as username, password, email, etc.
* Sensitive data, such as commercial or financial data, patients’ information
* Technical details of the website, such as the infrastructure

It mainly occurs when there are insecure configurations of the related technologies, such as default configurations when the hacker displays overly verbose error messages. The impacts could be very severe. For example, an online shop website leaking the credit cards information of their customers. However, the severity in some cases depends on the purpose of the hacker and what the hacker will do with the leaked information. [^10]

1. What this vulnerability could affect?

The hackers could take advantage of Heartbleed bug to gain the memory of the system when the system is using OpenSSL software in a version that the bug is not fixed. The secret keys during the traffic would be impacted directly. The whole communication would eavesdrop. In practice, Synopsys, Inc used this vulnerability to attack itself from outside. They finally stole from themselves the X.509 certificates secret keys, usernames, and passwords. From version 1.01 to 1.01f of OpenSSL did exist this vulnerability.

OpenSSL fixed this bug in version 1.01g on the 7th of April 2014.

1. 2 Public exploits

* [^11]
* 

There are 2 public exploits found on the exploit database. The author Jared Stafford disclaimed copyright to the source code. The 2 exploits directly demonstrate the ‘Heartbleed’ memory disclosure caused by OpenSSL TLS Heartbeat. [^12]

**Exploit Demo**

In this sample example, [www.scrooge-and-marley.com](http://www.scrooge-and-marley.com) will be the targeted server that we do the Heartbleed attack.

The tool used in this exploit

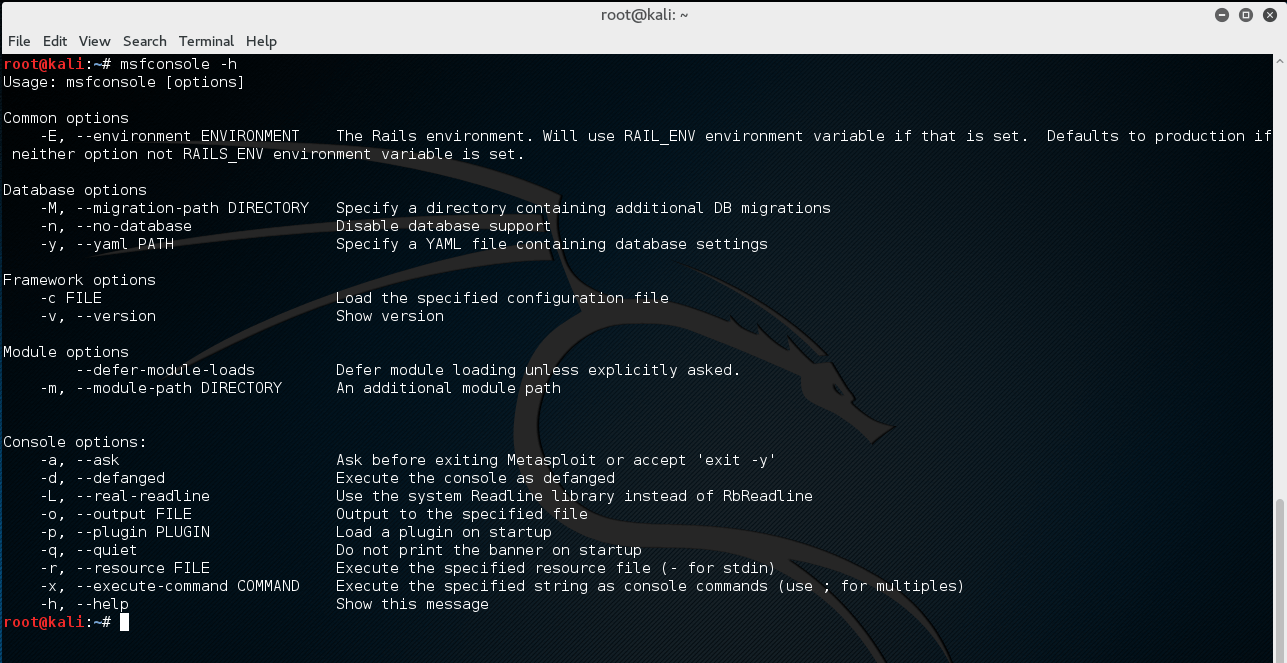
nmap:

“*Nmap ("Network Mapper") is a free and open-source utility for network discovery and security auditing.*” [^13]

Metasploit Framework (MSF) /msfconsole:

“*The Metasploit Framework is a Ruby-based, modular penetration testing platform that enables you to write, test, and execute exploit code.*” [^14]

The msfconsole is a command-line tool of the Metasploit Framework (MSF). (The following screenshot is the interface) The console provides users with all the options available in the MSF.

[^15]

Exploit Process:

1. Test the web site from the vulnerability

nmap -p 443 --script=ssl-heartbleed www.scrooge-and-marley.com

1. Use Metasploit to exploit

use auxiliary/scanner/ssl/openssl\_heartbleed

set RHOSTS www.scrooge-and-marley.com

set RPORT 443

set VERBOSE true

exploit

[^16]

Reference:

[^1] <https://www.balbix.com/insights/what-is-a-cve/>

[^2] <https://www.cve.org/About/Overview>

[^3]<https://www.csoonline.com/article/3204884/what-is-cve-its-definition-and-purpose.html>

[^4] <https://www.openssl.org/>

[^5] <https://heartbleed.com/>

[^6] <https://www.balbix.com/insights/understanding-cvss-scores/>

[^7] <https://www.cvedetails.com/>

[^8] <https://www.cvedetails.com/cve/CVE-2014-0160/>

[^9] <https://www.cvedetails.com/vulnerabilities-by-types.php>

[^10] <https://portswigger.net/web-security/information-disclosure>

[^11] https://www.exploit-db.com/exploits/32764

[^12] https://www.exploit-db.com/exploits/32745

[^13] <https://nmap.org/>

[^14] <https://docs.rapid7.com/metasploit/msf-overview/>

[^15] <https://www.offensive-security.com/metasploit-unleashed/msfconsole/>

[^16] <https://www.youtube.com/watch?v=-qzZIHJ0HLU>