Volume-4, Issue-3, March-2015 • ISSN No 2277 - 8160

Research Paper Computer Science

THE HEARTBLEED BUG: A RECENT VULNERABILITY IN OPENSSL

Mr. Sachin R. Ponde Assistant Professor, SIBACA, Lonavala

ABSTRACT

The Heartbleed Bug is a serious vulnerability in a popular OpenSSL cryptographic software library. This weakness allows stealing the protected information, by the SSL/TLS encryption used to secure the internet. SSL/TLS provides communication security and privacy over the internet for applications such as email, web applications, instant messaging (IM) and some virtual private networks (VPNs). This paper focuses on the this new bug in OpenSSL , risk involved with it, along with the mitigation.

KEYWORDS : Heartbleed, OpenSSL, SSL/TLS, CVE, VPN

INTRODUCTION

The OpenSSL Project is a collaborative effort to develop a robust, commercial-grade, full-featured, and Open Source toolkit implementing the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols as well as a full-strength general purpose cryptography library. The project is managed by a worldwide community of volunteers that use the Internet to communicate, plan, and develop the OpenSSL toolkit and its related documentation.

OpenSSL is based on the excellent SSLeay library developed by Eric A. Young and Tim J. Hudson. The OpenSSL toolkit is licensed under an Apache-style licence, which basically means that you are free to get and use it for commercial and non-commercial purposes subject to some simple license conditions. [1]

The Heartbleed bug allows anyone on the internet to read the memory of the systems protected by the vulnerable versions of the OpenSSL software. This compromises the secret keys used to identify the service providers and to encrypt the traffic, the names and passwords of the users and the actual content. This allows attackers to eavesdrop on communications, steal data directly from the services and users and to impersonate services and users.

RISK

The vulnerability could allow an attacker to potentially access a server's private cryptographic keys compromising the security of the server and its users. An attacker may be able to decrypt, spoof, or perform man-in-the-middle attacks on network communications that would otherwise be protected by encryption. Attackers could potentially impersonate bank services or users, steal login credentials, access sensitive email, or gain access to internal networks. Potential attacks are made feasible by the public availability of exploitation tools.

The Heartbleed bug allows anyone on the Internet to read the memory of the systems protected by the vulnerable versions of the OpenSSL software. This compromises the secret keys used to identify the service providers and to encrypt the traffic, the names and passwords of the users and the actual content. This allows attackers to eavesdrop on communications, steal data directly from the services and users and to impersonate services and users.

VULNERABILITY

An OpenSSL vulnerability was recently discovered that can potentially impact internet communications and transmissions that were otherwise intended to be encrypted.[2][3][4] According to open source reports, the vulnerability has existed since 2012, but was only recently discovered.[5] Cyber-criminals could exploit this vulnerability to intercept and decrypt previously encrypted information.[6] At this time there have not been any reported attacks or malicious incidents involving this particular vulnerability, but because it is a highly visible media topic, it is possible that cyber-criminals could exploit it in the future.

CVE-2014-0160 is the official reference to this bug. CVE (Common Vulnerabilities and Exposures) is the Standard for Information Security Vulnerability Names maintained by MITRE.

Many vendors have already begun issuing patches and have information posted on their websites and portals addressing the vulnerability and a plan of action. For example, Google, Facebook, and Yahoo implemented patches to fix the vulnerability as on 9 April 2014.[7] Additionally, all web browsers including Chrome, Firefox, and Internet Explorer on Windows OS all use Windows cryptographic implementation, not OpenSSL; however, consumers should still use caution until the vulnerability has been fully addressed.[8]

Status of different versions:

- OpenSSL 1.0.1 through 1.0.1f (inclusive) are vulnerable
- OpenSSL 1.0.1g -NOT vulnerable
- OpenSSL 1.0.0 -NOT vulnerable
- OpenSSL 0.9.8 -NOT vulnerable

In December 2011, this bug was introduced to OpenSSL and has been out naturally since OpenSSL release 1.0.1 on 14th of March 2012. OpenSSL 1.0.1g released on 7th of April 2014 fixes the bug.

MITIGATION

This vulnerability is not design flaw in SSL/TLS protocol specification. This is implementation problem of SSL/TLS protocol specification. It is programming mistake in popular OpenSSL library that provides cryptographic services such as SSL/TLS to the internet applications and services.

Encryption method is used to protect secrets that may affect your privacy or security if they leak. In order to manage recovery from this bug we have classified the compromised secrets to four categories: 1) Primary Key Material, 2) Secondary Key Material, 3) Protected Content and 4) Collateral (Security).

Primary key material is nothing but the encryption keys themselves. Leaked secret keys allow the attacker to decrypt any past and future traffic to the protected services and to impersonate the service at will. Any protection given by the encryption and the signatures in the X.509 certificates can be bypassed. Recovery from this leak requires patching the vulnerability, canceling of the compromised keys and reissuing and redistributing new keys. Even doing all this will still leave any traffic intercepted by the attacker in the past still vulnerable to decryption. All this has to be done by the owners of the services.

Secondary key material is the user information (user names and passwords) used in the vulnerable services. Recovery from this leak requires owners of the service first to restore trust to the service according to steps described above. After this users can start changing their passwords and possible encryption keys according to the instructions from the owners of the services that have been compromised. All session keys and session cookies should be invalidated and considered compromised.

Protected content is the actual content handled by the vulnerable services. It may be personal or financial details, private communication such as emails or instant messages, documents or anything seen

worth protecting by encryption. Only owners of the services will be able to estimate the likelihood what has been leaked and they should notify their users accordingly. Most important thing is to restore trust to the primary and secondary key material as described above. Only this enables safe use of the compromised services in the future.

Leaked collateral are other details that have been exposed to the attacker in the leaked memory content. These may contain technical details such as memory addresses and security measures such as betrayers used to protect against overflow attacks. These have only contemporary value and will lose their value to the attacker when OpenSSL has been upgraded to a fixed version.

This should be summarized as follows:
Server software vendors are working to incorporate a patched version of OpenSSL into their systems. Organizations including financial institutions should take the following steps, as appropriate:

- Ensure that third party vendors are aware of the vulnerability and take appropriate risk mitigation steps using OpenSSL on their systems
- Monitor the status of their vendors' efforts;
- Identify and upgrade vulnerable internal systems and services; and
- Follow appropriate patches through patch management practices and test to ensure a secure configuration of system.

CONCLUSIONS
OpenSSL is an open-source implementation of the Secure Sockets Layer and Transport Layer Security protocols specifications as an application. Organizations and Financial institutions may use OpenSSL in common network services such as Web servers, email servers, virtual private networks, instant messaging, and other applications.

A significant vulnerability has been found in OpenSSL that could allow an attacker to decrypt, spoof, or perform attacks on network communications that would otherwise be protected by encryption.

Following are the some recommendations to the user of OpenSSL :

- Change in passwords is strongly recommended, but only after the vulnerability has been fully addressed.
- Change in passwords before the vulnerability is fixed could still leave consumers vulnerable.
- Closely monitoring email accounts, bank accounts, social media accounts, and other online assets are strongly recommended.
- Once the vulnerability has been tackled, ensuring that visited websites requiring personal information such as login information or credit card information all are secure with the HTTPS identifier in the address bar.

REFERENCES

[1] https://www.openssl.org/ | [2] https://www.openssl.org/news/secadv_20140407.txt | [3} https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160 | [4] iSight Partners | [5] SANS OpenSSL Vulnerability | [6] http://www.cio.com/article/751207/ Vendors_and_Administrators_Scramble_to_Patch_OpenSSL_Vulnerability?taxonomyId=3089 | [7] http://www.cnet.com/how-to/which-sites-have-patched-the-heartbleed-bug/ | [8] SANS OpenSSL Vulnerability | [9] U.S. CERT: OpenSSL 'Heartbleed' Vulnerability, CVE-2014-0160 https://www.us-cert.gov/ncas/alerts/TA14-098A | [10] http://news.unchealthcare.org/empnews/2014/april-17/cyber-alert-heartbleed-vulnerability | [11] http://www.chabotcomputers.com/ | [12] http://fcw.com/articles/2014/04/14/nefarious-actors-moving-to-exploit-heartbleed.aspx |