Threat Advisory Bulletin

Vigilant by Deloitte.

Issue 1.2 April 9, 2014

Heartbleed bug can expose web application data

- Enables unauthorized access to some data residing in system memory
- May impact a very wide range of servers and appliances
- Upgrading to patched OpenSSL version 1.0.1g is strongly advised

Summary

On April 7, 2014, researchers exposed the Heartbleed bug (CVE-2014-0160). The Heartbleed bug is a vulnerability in the widely used OpenSSL software library, which implements basic cryptography and other functions. OpenSSL is the standard library used for SSL/TLS implementation and is utilized by most major web servers.

How It Works

Vulnerable versions of OpenSSL shipped with a wide variety of applications and operating systems. Hardware applications, such as SSL-based VPNs, are also affected. The bug allows an attacker to access up to 64 kilobytes of unallocated memory from a server by exploiting a flaw in the implementation of the SSL/TLS heartbeat extension. Although the attacker will have access to any data formerly held in that unallocated memory chunk, they cannot determine which section of memory they receive. Therefore, the information received may be either useless or very sensitive, simply based on chance.

Examples of the information stored in memory include primary and secondary keys used to encrypt and decrypt private data. Additionally, attackers may receive usernames, passwords, private documents, financial information and private communications, such as emails or instant messages. This exploit operates solely by accessing memory present on the server. It is not a remote code exploit or Denial of Service attack.

OpenSSL versions 1.0.1 through 1.0.2-beta are compromised. This includes version 1.0.1f which was the most recent version in production until April 7, 2014. The earliest version affected, 1.0.1-beta1, was created on February 22, 2012. This indicates the bug was unpatched and exploitable for over two years. The earlier 0.9.8 and 1.0.0 branches of OpenSSL were unaffected.

Actions and Remediation

OpenSSL has released a new version of its software, 1.0.1g, with a patch to resolve the problem. Organizations should make a risk-based decision to:

- Upgrade affected servers and devices immediately. External facing servers hosting high-risk applications or sensitive data should be prioritized.
- Avoid connecting to vulnerable websites until the problem has been mitigated. It may be advisable to avoid logging into public web services until verifying that the website has been updated, and then to change passwords after the website has been updated.

Once affected devices are patched, a determination should be made whether to revoke and replace SSL keys. Given the time and effort this may require, organizations may want to undertake this selectively, weighing the level of asset criticality. In cases where it is not practical to immediately modify business-critical systems, consider using alternative means, such as Web application firewalls, intrusion prevention systems (IPS), or intrusion detection systems (IDS) to provide additional controls.

Emerging Threats has assembled a list of IDS signatures associated with the Heartbleed bug. Python Proof of Concept (PoC) code can be used to test whether a site is running a vulnerable version of OpenSSL. This is an alternative to public websites if companies want to test independently. Links to both are found in “Additional resources” in the right column.

In Context

Other related vulnerabilities

- **DSA- 1571- 1**: OpenSSL Predictable Random Number Generator (May 2008)
- **BREACH**: TLS Exploit (August 2013)

This vulnerability highlights that strong asset management practices, in this case tracking versions of system software in use, particularly when rated for business criticality, can help speed remediation processes.

About us

Deloitte’s Vigilant Cyber Science Team (CST) helps complex organizations gain insight about cyber threats and risk posture so they can be more proactive in protecting assets and mitigating technology-related risks. The CST:

- Maintains an enriched threat feed for enterprise threat detection
- Conducts intelligence research to provide guidance on detection, protection and prevention methods
- Develops analytic tools and methodologies to help complex organizations turn high volumes of data into actionable insight for improved business risk mitigation.

Additional resources

- For general information: **http://heartbleed.com**
- **Emerging Threats IDS Signatures**
- **Python PoC Code**

Contacts

Vikram Bhat
Principal, Cyber Risk Services
Deloitte & Touche LLP
vbhat@deloitte.com

Christopher Stevenson
Head of Research and Development
Vigilant by Deloitte
Deloitte & Touche LLP
chstevenson@deloitte.com

Lance James
Head of Cyber Intelligence
Deloitte & Touche LLP
lancejames@deloitte.com
+1 760.262.4141

As used in this document, “Deloitte” means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see **www.deloitte.com/us/about** for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

This bulletin contains general information only and Deloitte is not, by means of this bulletin, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This bulletin is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this bulletin.

DeloitteNet | **Security** | **Legal** | **Privacy**

30 Rockefeller Plaza
New York, NY 10112-0015
United States

PARALYMPICS Official Professional Services Sponsor

Professional Services means audit, tax, consulting and financial advisory services.