Heartbleed
OpenSSL vulnerability

On April 7, 2014, a serious vulnerability in the popular OpenSSL cryptographic software library was publically disclosed. At the time of disclosure, it was estimated that over 66% of the Internet's web servers use the OpenSSL library. This software vulnerability in OpenSSL has been integrated in popular services such as Apache HTTP Server, Nginx, and OpenVPN for over two years.

The OpenSSL developers were alerted to this software bug and released a security patch prior to the public disclosure of the issue. Due to the critical severity and widespread prevalence, PwC has developed a methodology to assist our clients in identification and suggested remediation.

What is the OpenSSL Heartbleed Bug?

The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing information that is normally encrypted by SSL/TLS encryption.

What type of sensitive information can be compromised from a vulnerable server?

This vulnerability allows an attacker to pull 64KB of arbitrary memory from the server. There is a possibility that sensitive information can be stored in this memory location, and therefore any data on the server could be compromised. In practice, operating systems tend to allocate memory linearly and therefore there is high probability information relevant to this TLS session is located within the visible 64KB window. In worst-case scenarios, server private keys, session cookies, or passwords could be at risk.

How does the Heartbleed exploit work?

The malicious user modifies the heartbeat request by making the payload as small as possible, as an example 1 byte, and more importantly they change the size parameter to 65535 bytes (or 64KB, the payload's maximum possible size). What happens then is that the vulnerable web server responds to the request, however, because it assumes that the size of the payload is really 65535 bytes without verifying the actual size, the webserver then returns the original 1byte of the payload along with the next 65534 bytes stored in memory, believing that all 65535 bytes are a part of the original payload.

What is the Impact?

If the 64KB of data that the malicious user pulled contains private key information, then the malicious user would be able to not only decrypt currently captured traffic, but also decrypt previously captured traffic. The 64KB of memory could also contain sensitive information such as email addresses, passwords, PII, etc.. An attacker can gain access to this memory space as it changes by repeatedly issuing requests. Over time, the attacker will be able exfiltrate large quantities of potentially sensitive data.

How can one test if a system is vulnerable?

System administrators can check if a system is vulnerable by locally logging into the server and identifying the OpenSSL version number. Additionally, systems can be checked by scanning for the vulnerability. PwC has developed a methodology to validate whether or not systems are vulnerable/exploitable.

What versions of the OpenSSL are affected?

Status of different versions:

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

The bug was introduced to OpenSSL in December 2011 and has been in the wild since OpenSSL release 1.0.1 on March 14, 2012. OpenSSL 1.0.1g, released on April 7, 2014, fixes the bug.

How can OpenSSL be fixed?

The OpenSSL team has issued a new version, 1.0.1g, with the Heartbleed fix implemented. Version 1.0.1g or newer should be used. If this is not possible, software developers can recompile OpenSSL with the handshake removed from the code with the compile time option -DOPENSSL_NO_HEARTBEATS.

Do certificates need to be reissued?

Yes, since private keys could have been stolen all certificates should be revoked, regenerated, and redistributed. If an attack has a server's private key, the public-key crypto implementation will be compromised allowing SSL traffic to be intercepted.

How can PwC help you?

PwC has the required experience and credentials to assist clients various information technology and information security areas. In this particular case, we have developed a methodology to assist our clients in identification and suggested remediation. We have the tools to validate whether or not your systems are vulnerable/exploitable from the Internet and we can help you to identify and validate any other systems on your internal network.

Have you assessed and addressed the information leakage risks that your business is facing?

Patrick MacGloin
Director
+971 (0) 4304 3418
patrick.macgloin@ae.pwc.com

*Potential False Positives - It is important to note that some Linux/Unix distributions have fixed this bug in their own OpenSSL branches. For example, Debian's OpenSSL 1.0.1e-2+deb7u5 is in the above vulnerable version range, however 1.0.1e-2+deb7u5 has been patched. If you are performing manual verification, check your distributions security advisory website to see if a similar false positive scenario exists.

http://pwc.to/1ibmCCW

www.pwc.com/me

PwC firms help organisations and individuals create the value they're looking for. We're a network of firms in 157 countries with close to 184,000 people who are committed to delivering quality in assurance, tax and advisory services. Tell us what matters to you and find out more by visiting us at http://www.pwc.com/

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.