CYBER SECURITY BULLETIN

Cyber Security Bulletin Number: 002

Type of Cyber Threat:

The Heartbleed Bug: a serious vulnerability in the popular OpenSSL cryptographic software library.

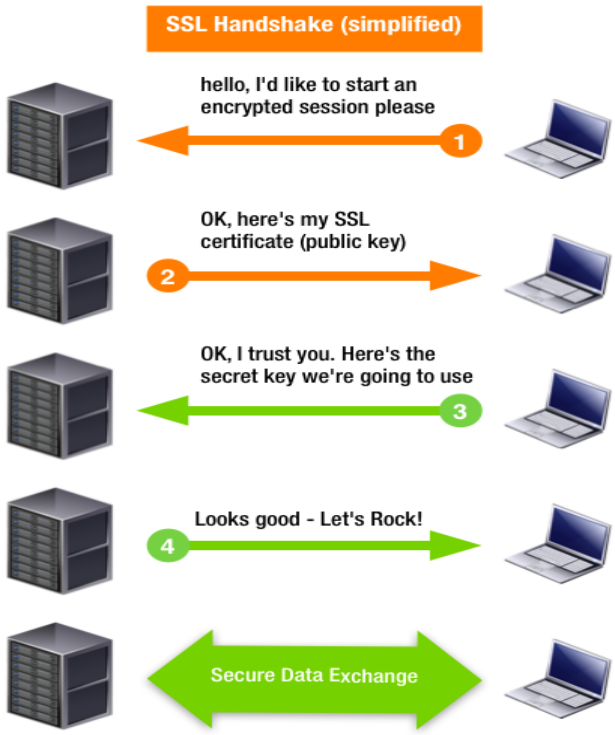
Date Monitored: 01 April 2014

Description:

The Heartbleed Bug is a weakness that allows stealing of information protected by the SSL/TLS, encryption used to secure data exchange in the Internet. In normal conditions, 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 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.

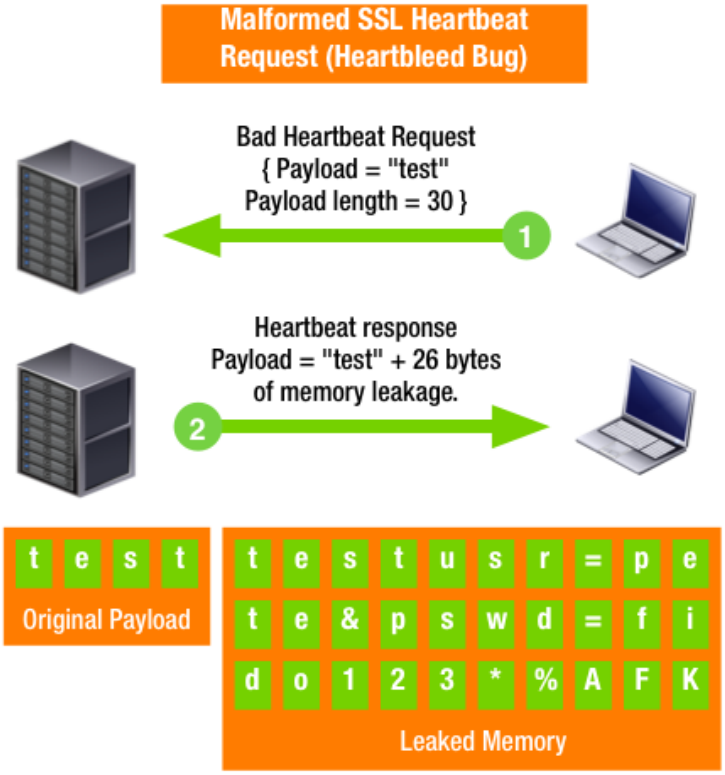
Analysis:



The heartbeat (where the name of the bug came from) extension for Transport Layer Security (TLS) was designed so that once secure communications were established between a client and server, the client could send keep-alive requests to the servers to make sure everything was still OK. The heartbeat request includes two (2) important parameters:

1) A heartbeat message (which could be anything "test" for example) – called payload.
2) The length of the payload (which in the case of our example payload would be simply 4) – called payload length.

The heartbleed bug meant that a request including a small payload but telling the server the payload_length is much larger would force the server to send a response including the contents of raw memory beyond the original payload. This type of bug is known as a memory leak and presents serious security implications. This is illustrated below.



Suggested Actions:

Change your password when the web server you are connecting to have already been patched. If the server concerned was not yet patched, then any new password would be equally vulnerable to leakage.

The only way to be sure it's safe to reset your password is either to wait for the server owner to announce they have patched the problem or to test it yourself. Using a

public testing service such as www.ssllabs.com/ssltest (https://www.ssllabs.com/ssltest) will test for the bug. (However the legality of such tests has been called into question so do so at your own risk.)

Note:

Connection to the Philippine Army Information Systems requires the use of PANet, our own private network also called an intranet. Access to our different Information Systems is through our intranet and not on the internet.

References: http://krystal.co.uk/blog/2014/04/the-openssl-heartbleed-bug-simplified/