ThreatCloud Intelligence Analysis:
Heartbleed: A Look into the new Threat on the Block

16 April 2014

Check Point Malware Research Group

What is Heartbleed and how does it work?

Earlier this month, the Security teams at Codenomicon and Google Security discovered the critical security bug known as Heartbleed (CVE-2014-0160). This vulnerability has been found in versions 1.0.1 through 1.0.1f of the popularly used OpenSSL cryptographic software, providing an easy path for attackers to access very sensitive information from popular websites and applications on the internet, including Yahoo!, Google, Gmail, Yahoo! Mail, Instagram, Pinterest, Netflix and many more. It is important to note that in addition to our everyday websites and internet applications, Heartbleed also affects internal enterprise web server platforms and any network service that uses the vulnerable versions of OpenSSL thus leaving enterprises that use affected tools and applications open to these attacks. (Please be aware that many of the mentioned affected sites and applications have already implemented patches for this vulnerability. Find more information here.)

According to Netcraft's April 2014 Web Server Survey, OpenSSL is an open-source software package used by over 66% of websites on the internet to encrypt sensitive information such as passwords, logins, personal information, and encryption keys. In addition to securing HTTPS connections, OpenSSL is also widely used to secure other protocols like FTPS, SMTPS and IMAPS. In December 2011, OpenSSL version 1.0.1 implemented what was called the "Heartbeat Extension" for the TLS/DTLS protocols (RFC 6520). Heartbeat Extension protocol was created as a way to keep the TLS/DTLS (transport layer security protocols) connections alive without continuous data transfer.

As it happens, the Heartbleed bug is found on all versions of the OpenSSL that use the Heartbeat extension. With this bug, attackers can use vulnerable servers to repeatedly scrape up to 64 KB of sensitive information at a time from the computer's memory. What's more concerning is that all this can be done by an attacker without leaving a trace.

The Heartbleed bug, although recently revealed to the general public, has been around for almost 2 years now. This could mean that a number of encryption keys, logins, and passwords could very well already be exposed to attackers who have tried to exploit this vulnerability.

Recommendations: Protecting your organization

Check Point Customers

1. Check Point network security products are not affected by Heartbleed because they utilize a non-vulnerable version of OpenSSL.

2. Check Point has multiple protections against this vulnerability including the implementation of HTTPS inspection (introduced in 2011 with R75.20) which automatically prevents

Heartbleed traffic and IPS protections released on April 9th 2014 to detect and block exploits from Heartbleed. For more information on these protections, see:

- Sk100173 - Check Point response to OpenSSL vulnerability (CVE-2014-0160)
- Sk100246 - Check Point IPS Protections for OpenSSL Heartbleed vulnerability (CVE 2014-0160)

Non Check Point Customers

1. Determine if your security infrastructure such as Firewall, IPS, etc. is vulnerable to Heartbleed
2. Determine if vulnerable versions of OpenSSL is used in any of your essential network services and public applications
3. Consider getting a free network assessment today, in addition to deploying Check Point's security gateways and the IPS Software Blade solution

All Organizations

In order to reduce the risk of being affected by Heartbleed, all organizations should follow the recommended steps.

Network and System Administrators

1. Patch your systems with version 1.0.1g of OpenSSL
2. Acquire and install a new SSL certificate for your website
3. Revoke the old SSL certificate for your website
4. Enforce a password reset for all employees and customers on their next login
5. Provide customers with an FAQ on Heartbleed as it relates to your website

End-Users

1. Verify that the websites you use are clear of this vulnerability by going to lastpass.com/heartbleed
2. Consider using a browser plugin to check for a website's Heartbleed risk
3. Change your passwords on sites known to be compromised after the site has been fixed
4. Set your browser to warn you when visiting a site with a revoked certificate, test by visiting https://www.cloudflarechallenge.com/heartbleed
5. Be cautious of suspicious emails, URLs and files

To learn more about this vulnerability, please visit heartbleed.com and openssl.org.