COMPUTER SECURITY BULLETIN

Risk/Impact Rating: SERIOUS

< Heartbleed OpenSSL Bug >

CSB17-005

Description:

Heartbleed (CVE-2014-0160) was a serious bug in the OpenSSL's implementation of the TLS/DTLS heartbeat extension that allowed attackers to read portions of the affected server's memory, potentially revealing users data that the server isn't intended to reveal.

This year, due to unpatched OpenSSl instances, about 200,000 devices remain exploitable.

The countries most affected are:

- United States
- Korea
- China
- Germany
- France
- Russian Federation
- United Kingdom
- India
- Brazil
- Italy.

This flaw is more critical and probably the biggest Internet flaw in recent history as it left the contents of a server's memory, where the most sensitive data is stored, exposed to the attackers.

It access up to 64 kilobytes of server memory, but perform the attack over and over again to get lots of information. An attacker could get not just usernames and passwords, but also "cookie" data that Web servers and browsers use to track individuals and ease log-in.

Doing the attack repeatedly could yield more serious information, like a site's private SSL key, used to encrypt traffic. With that key, someone could run a fake version of a Web site and use it to steal all other kinds of information, like credit card numbers or private messages.

Recommendations / Solutions / How To's:

1. Patching: Update your software to the latest versions of OpenSSL;
2. Creation of New Private Keys: Creating new private keys will prevent an attacker, who already exploited the flaw before patching, from being able to spy on your encrypted; and
3. Reissuance of Security Certificates: This step will eliminate the ability of any attacker to spoof organizations and fool or phish their customers.

References:

http://thehackernews.com/2017/01/heartbleed-openssl-vulnerability.html

https://www.cnet.com/news/heartbleed-bug-what-you-need-to-know-faq/

https://www.symantec.com/security_response/attacksignatures/detail.jsp?asid=27517