



**State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory**

April 8, 2014

The following cyber advisory was issued by the State of Alaska and was intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

ADVISORY NUMBER:

SA2014-022

DATE(S) ISSUED:

04/08/2014

SUBJECT:

OpenSSL TLS 'heartbeat' Extension Information Disclosure Vulnerability

EXECUTIVE SUMMARY:

A vulnerability has been discovered in OpenSSL's implementation of the TLS 'heartbeat' extension that could allow for the disclosure of sensitive information. OpenSSL is an open-source implementation of the SSL protocol used by a number of other projects. SSL (Secure Sockets Layer) is a protocol that ensures secure communication over the Internet via encryption. This issue could allow an attacker to compromise the private key and other sensitive data stored in memory.

THREAT INTELLIGENCE:

Proof-of-concept code has been released. This vulnerability was first included in OpenSSL release 1.0.1 on 14th of March 2012. OpenSSL 1.0.1g released on 7th of April 2014 fixes the issue. Software products known to be using OpenSSL are the open source web servers Apache and nginx. According to Netcraft's April 2014 Web Server Survey (<http://news.netcraft.com/archives/2014/04/02/april-2014-web-server-survey.html>) of 958,919,789 websites, the combined market share of these products on the Internet was over 66%.

SYSTEMS AFFECTED:

- OpenSSL versions 1.0.1 to 1.0.1f

RISK:

Government:

- Large and medium government entities: High
- Small government entities: High

Businesses:

- Large and medium business entities: High
- Small business entities: High

Home users: High

TECHNICAL SUMMARY:

An information disclosure vulnerability has been discovered in OpenSSL's implementation of the TLS 'heartbeat' extension that could allow for an attacker to obtain sensitive information residing in memory. This issue occurs because OpenSSL fails to conduct proper bounds checks when handling TLS 'heartbeat' packets. Up to 64KB of memory from either the client or the server can be recovered by an attacker and could allow an attacker to compromise the private key and other sensitive data in memory. It is known to be used on various platforms including Linux and Mac OS X.

- OpenSSL 1.0.1g is NOT vulnerable.
- OpenSSL 1.0.0 branch is NOT vulnerable
- OpenSSL 0.9.8 branch is NOT vulnerable

More information about this threat as well as a web-based testing tool is available at: <http://heartbleed.com>

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply appropriate updates provided by the OpenSSL project to affected systems immediately after appropriate testing.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.

REFERENCES:

OpenSSL:

https://www.openssl.org/news/secadv_20140407.txt

Heartbleed:

<http://heartbleed.com>

Security Focus:

<http://www.securityfocus.com/bid/66690>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160>