The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is 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.

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

http://www.us-cert.gov/tlp/

DATE(S) ISSUED:

03/19/2015

SUBJECT:

Multiple Vulnerabilities in OpenSSL Could Lead to Denial of Service Conditions

OVERVIEW:

Multiple vulnerabilities have been discovered in OpenSSL. OpenSSL is an open-source implementation of the SSL protocol used by a number of applications and products. SSL (Secure Sockets Layer) is a protocol that ensures secure communication over the Internet via encryption. Successful exploitation of these vulnerabilities may result in denial of service conditions.

THREAT INTELLIGENCE

There are no reports of these vulnerabilities being exploited in the wild.

VERSIONS AFFECTED:

OpenSSL 1.0.2 users should upgrade to 1.0.2a.
OpenSSL 1.0.1 users should upgrade to 1.0.1k.
OpenSSL 1.0.0 users should upgrade to 1.0.0p.
OpenSSL 0.9.8 users should upgrade to 0.9.8zd.

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:

Multiple vulnerabilities have been discovered in OpenSSL. The details of these vulnerabilities are as follows:

- A Null pointer dereferencing issue may result in denial of service conditions (CVE-2015-0208, CVE-2015-0288,CVE-2015-0289, CVE-2015-0291).
- RSA export ciphersuites are prone to a man-in-the-middle (MITM) attack (CVE-2015-0204).

- A defect in the implementation of "multiblock" may result in denial of service conditions (CVE-2015-0290).
- A defect in the implementation of DTLSv1 Segmentation fault in DTLSv1_listen changes the ClientHello to act statefull (CVE-2015-0207).
- ASN1_TYPE_cmp may result in denial of service conditions when comparing ASN.1 boolean types (CVE-2015-0286).
- Reusing a structure in ASN.1 parsing may result in memory corruption (CVE-2015-0287).
- An issue in the Base64 decoding may cause memory corruption (CVE-2015-0292).
- Servers supporting SSLv2 and enable export cipher suites may be susceptible to denial of service conditions (CVE-2015-0293).
- A server may be susceptible to denial of service conditions when processing DHE ciphersuites (CVE-2015-1787).
- OpenSSL client may be susceptible to an unseeded PRNG handshake (CVE-2015-0285)
- Use-after-free following d2i_ECPrivatekey error denial of service conditions or memory corruption (CVE-2015-0209).

Successful exploitation could result in an attacker compromising data security, potentially allowing access to confidential data, or could compromise processing resources in a user's computer.

RECOMMENDATIONS:

The following actions should be taken:

- After appropriate testing, apply appropriate updates to vulnerable systems immediately.
- 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_20150319.txt

CVE:

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0204
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0207
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0208
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0209
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0285
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0286
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0287
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0288
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0289
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0290
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0292
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0293
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1787
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2091