

*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:**

05/03/2016

**SUBJECT:**

Multiple Vulnerabilities in OpenSSL Could Allow for Arbitrary Code Execution

**OVERVIEW:**

Multiple vulnerabilities have been discovered in OpenSSL, the most severe of which could allow for arbitrary code execution. OpenSSL is an open-source implementation of the SSL and TLS protocols used by a number of applications and products. SSL (Secure Sockets Layer) and TLS (Transport Layer Security) are protocols which ensure secure communication over the Internet via encryption. Successful exploitation of these vulnerabilities could result in arbitrary code execution in the context of the application, an attacker gaining elevated privileges, gaining sensitive information or bypassing security restrictions. Failed exploit attempts will most likely result in denial-of-service conditions.

**THREAT INTELLIGENCE:**

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

**SYSTEM AFFECTED:**

- OpenSSL versions 1.0.2 prior to 1.0.2h
- OpenSSL versions 1.0.1 prior to 1.0.1t

**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:**

OpenSSL is prone to multiple vulnerabilities, the most severe of which could allow for arbitrary code execution. The vulnerabilities are as follows:

- Multiple arbitrary code execution vulnerabilities exist in the 'EVP\_EncodeUpdate()' & 'EVP\_EncryptUpdate()' functions as they fail to adequately bounds-check user supplied data before copying it into an insufficiently sized buffer. (CVE-2016-2105, CVE-2016-2106)

- A memory exhaustion vulnerability in BIO functions when they parse ASN.1 data. (CVE-2016-2109)
- Multiple information disclosure vulnerabilities exist in OpenSSL. (CVE-2016-2107, CVE-2016-2176)
- Successful exploitation of these vulnerabilities could result in arbitrary code execution in the context of the application, an attacker gaining elevated privileges, gaining sensitive information or bypassing security restrictions. Failed exploit attempts will most likely result in denial-of-service conditions.

#### **RECOMMENDATIONS:**

The following actions should be taken:

- Apply appropriate updates provided by OpenSSL and/or applicable vendors to vulnerable systems, immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Do not use the same OpenSSL private keys across multiple systems and update OpenSSL keys periodically.
- Disable legacy support for SSLv2 and v3, and TLS 1.0 and 1.1. Migrate fully to TLS 1.2 where possible after appropriate testing.

#### **REFERENCES:**

##### **OpenSSL:**

<https://www.openssl.org/news/secadv/20160503.txt>

##### **CVE:**

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2176>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2109>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2107>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2106>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2105>

#### **TLP: WHITE**

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

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