

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:**

09/19/2016

**SUBJECT:**

Vulnerability in OpenSSL Could Allow for Arbitrary Code Execution

**OVERVIEW:**

A vulnerability has been discovered in OpenSSL 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 could result in the attacker executing arbitrary code in the context of the user running the affected application. Failed exploit attempts will most likely result in denial-of-service conditions.

**THREAT INTELLIGENCE:**

There are currently no reports of the vulnerability being exploited in the wild.

**SYSTEM AFFECTED:**

- OpenSSL versions prior to 1.1.0

**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 a vulnerability which could allow for arbitrary code execution. The vulnerability is as follows:

- OpenSSL is prone to an integer-overflow vulnerability because of an out-of-bound write error. Specifically, this issue affects the 'MDC2\_Update()' function of 'crypto/mdc2/mdc2dgst.c' source file.

Successful exploitation could result in the attacker executing arbitrary code in the context of the user running the affected application. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights. Failed exploit attempts will 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.

**REFERENCES:**

**CVE:**

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6303>

**TLP: WHITE**

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

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