



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

March 02, 2016

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:

SA2016-035

DATE ISSUED:

03/02/2016

SUBJECT:

Multiple Vulnerabilities in OpenSSL Could Allow for Security Bypass

OVERVIEW:

Multiple vulnerabilities have been discovered in OpenSSL, the most severe of which could result in a bypass of security features. 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 allow an attacker to bypass certain security measures, cause denial of service conditions, or lead to information disclosure.

THREAT INTELLIGENCE:

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

SYSTEM AFFECTED:

- OpenSSL versions prior to 1.0.2g and 1.0.1s

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: Low

TECHNICAL SUMMARY:

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

- Side channel attack on modular exponentiation could lead to a local security bypass vulnerability. (CVE-2016-0702)
- Divide-and-conquer attack on SSLv2 could lead to an information disclosure vulnerability. (CVE-2016-0703)
- Failure to properly implement Bleichenbacher protection for export cipher suites could lead to information disclosure. (CVE-2016-0704)
- Double-free bug in DSA code could lead to a denial of service condition. (CVE-2016-0705)
- Heap corruption in the BN_hex2bn function could lead to denial of service conditions. (CVE-2016-0797)
- Memory leak in SRP database lookups could lead to a denial of service condition. (CVE-2016-0798)
- Multiple integer overflow vulnerabilities could lead to denial of service conditions. (CVE-2016-0799)
- Cross-protocol attacks on TLS using SSLv2 could lead to a security bypass vulnerability (a.k.a. DROWN). (CVE-2016-0800)

The DROWN Attack (CVE-2016-0800) allows an attacker to compromise HTTPS streams that rely on SSL, and view the information being transmitted, when SSLv2 is installed on the server. SSLv2 and v3 were deprecated in 2011 and 2015 respectively and as such should be disabled. Migrating to exclusive TLS support will mitigate the Drown Attack.

Successful exploitation of these vulnerabilities could allow an attacker to bypass certain security measures, cause denial of service conditions, or lead to information disclosure.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply appropriate patches provided by OpenSSL 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 migrate fully to TLS.
- Check websites for vulnerability to the DROWN attack at <https://drownattack.com>.

REFERENCES:

OpenSSL:

<https://www.openssl.org/news/secadv/20160301.txt>

DrownAttack:

<https://drownattack.com>

<https://drownattack.com/drown-attack-paper.pdf>

CVE:

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0702>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0703>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0704>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0705>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0797>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0798>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0799>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0800>