



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

October 15, 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:

SA2014-069

DATE(S) ISSUED:

10/15/2014

SUBJECT:

Vulnerability in SSLv3 Could Allow Information Disclosure

EXECUTIVE SUMMARY:

A vulnerability exists within the SSL version 3.0 protocol allowing an attacker to hijack and decrypt session cookies that are utilized between a user's web browser and the web site. Secure Sockets Layer (SSL) is a cryptographic protocol that is designed to provide secure network communication using X.509 certificates. This could lead to attackers temporarily impersonating web site visitor account logins and/or online payment systems.

THREAT INTELLIGENCE:

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

SYSTEM AFFECTED:

- Any client or Web Server supporting SSLv3 protocol

RISK:

Government:

- Large and medium government entities: **Moderate**
- Small government entities: **Moderate**

Businesses:

- Large and medium business entities: **Moderate**
- Small business entities: **Moderate**

Home users: Low

TECHNICAL SUMMARY:

A vulnerability exists within the SSL version 3.0 protocol due to improper cipher-block chaining (CBC) mode decryption used within the block ciphers allowing an attacker to hijack and decrypt session cookies that are utilized between a user's web browser and

the web site. This could lead to attackers obtaining enough information to temporarily impersonate web site visitor account logins and/or online payment systems. Please note that the website and the end-user's system must support SSLv3, and the attacker must be able to intercept and modify the network traffic in order to successfully perform the Man-in-the-Middle (MITM) attack to exploit this vulnerability.

Successful MITM attacks could lead to the attacker having temporary control over the attacked user's web session through session hijacking.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Disable SSL3 support both server side and within the client browser settings
- Keep all operating system, applications and essential software up to date to mitigate potential exploitation by attackers.
- Update all plugins used by the webserver and disable/remove all unused plugins.
- Ensure that systems are hardened with industry-accepted guidelines.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack

REFERENCES:

OpenSSL:

<https://www.openssl.org/~bodo/ssl-poodle.pdf>

Google:

<http://googleonlinesecurity.blogspot.com/2014/10/this-poodle-bites-exploiting-ssl-30.html>

Threatpost:

<https://threatpost.com/new-poodle-ssl-3-0-attack-exploits-protocol-fallback-issue/108844>

CSO Online:

<http://www.csoonline.com/article/2833912/application-security/dreaded-ssl3-bug-no-monster-only-a-poodle.html>

WIRED:

<http://www.wired.com/2014/10/poodle-explained/>

SANS:

<https://isc.sans.edu/forums/diary/OpenSSL+SSLv3+POODLE+Vulnerability+Official+Release/18827>