Enterprise Technology Services

State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory

May 15, 2008

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.

STATE OF ALASKA ADVISORY NUMBER:

2008-013

DATE(S) ISSUED:
May 15, 2008

SUBJECT:
CRITICAL DEBIAN/UBUNTU SECURITY VULNERABILITY

OVERVIEW:
Debian and Ubuntu have released multiple security advisories to address a vulnerability in their OpenSSL package and other cryptographic application packages that rely on it. A weakness exists in the random number generator used by the OpenSSL package included with the Debian GNU/Linux operating system and derivative systems that causes the generated numbers to be predictable. As a result of the vulnerability, the keys generated using the flawed OpenSSL package may be weak. Exploitation of these vulnerabilities may allow a remote, unauthenticated attacker to conduct brute force attacks and obtain sensitive information.

US-CERT is following reports that indicate there are working exploits available that allow brute force attacks against vulnerable keys. US-CERT strongly encourages users to review the following information and links. Affected agencies/organizations should apply the vendor updates and regenerate vulnerable keys.

US-CERT has published a Current Activity entry and Vulnerability Note detailing these advisories. They are available at:
http://www.us-cert.gov/current/#debian_openssl_vulnerability
http://www.kb.cert.org/vuls/id/925211

In addition, SANS Internet Storm Center has raised their INFOCon level to Yellow as a result of this issue. You can read more at http://isc.sans.org/.

Below are the contents from the US-CERT VULNERABILITY NOTE -VU#925211

DEBIAN AND UBUNTU OPENSSL PACKAGES CONTAIN A PREDICTABLE RANDOM NUMBER GENERATOR

Overview:
A vulnerability in the OpenSSL package included with the Debian GNU/Linux operating system and its derivatives may cause weak cryptographic keys to be generated.

I. Description
A weakness exists in the random number generator used by the OpenSSL package included with the Debian GNU/Linux operating system and derivative systems that causes the generated numbers to be predictable. As a result of this weakness, certain encryption keys are much more common than they should be. This vulnerability affects cryptographic applications that use keys generated by the flawed versions of the OpenSSL package. Affected keys include SSH keys, OpenVPN keys, DNSSEC keys, and key material for use in X.509 certificates and session keys used in SSL/TLS connections. Any of these keys generated using the affected systems on or after 2006-09-17 may be vulnerable. Keys generated with GnuPG or GNUTLS on the affected systems are not vulnerable because these applications use their own random number generators and not the one from the flawed version of OpenSSL.

Note that this vulnerability is specific to Debian, Ubuntu Linux and other Debian-derived operating systems. Other systems can be indirectly affected if weak keys generated by the vulnerable systems are imported into them.

II. Impact
A remote, unauthenticated attacker with minimal knowledge of the vulnerable system and the ability to conduct a brute force attack against an affected application may be able to guess secret key material. Secondary impacts include authenticated access to the system through the affected service or the ability to perform man-in-the-middle attacks.

SYSTEMS AFFECTED:

- All versions of Debian/Ubuntu

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

RECOMMENDATIONS:
We recommend the following actions be taken:

Apply a patch from the vendor and regenerate key material Patches have been release by the affected vendors. Users are encouraged to review the security advisories listed below and apply the updates.

Due to the nature of the flaw, any key material generated by the vulnerable versions of the OpenSSL package should be considered fatally defective. After the software updates are applied, this key material must be regenerated with the updated version of the software.

Debian Security Advisory DSA-1571-1 - http://www.debian.org/security/2008/dsa-1571
Debian Security Advisory DSA-1576-1 - http://www.debian.org/security/2008/dsa-1576
Ubuntu Security Notice USN-612-1 – http://www.ubuntu.com/usn/usn-612-1
Ubuntu Security Notice USN-612-2 - http://www.ubuntu.com/usn/usn-612-2
Ubuntu Security Notice USN-612-3 - http://www.ubuntu.com/usn/usn-612-3
Ubuntu Security Notice USN-612-4 - http://www.ubuntu.com/usn/usn-612-4
Ubuntu Security Notice USN-612-5 - http://www.ubuntu.com/usn/usn-612-5
Ubuntu Security Notice USN-612-6 - http://www.ubuntu.com/usn/usn-612-6

REFERENCES:

Debian:

http://security.debian.org/project/extra/dowkd/dowkd.pl.gz
http://www.debian.org/security/key-rollover/

Metasploit:

http://metasploit.com/users/hdm/tools/debian-openssl/