



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

September 21, 2012

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:

SA2012-059

DATE(S) ISSUED:

09/21/2012

SUBJECT:

Multiple Vulnerabilities in Apple Mac OS X

OVERVIEW:

Multiple vulnerabilities have been discovered in Apple's Mac OS X and Mac OS X Server that could allow remote code execution. Mac OS X is a desktop operating system for the Apple Mac. Mac OS X Server is a server operating system for the Apple Mac.

These vulnerabilities may be exploited if a user visits or is redirected to a specially crafted web page or when a user opens a specially crafted file. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

- Apple Mac OS X 10.6
- Apple Mac OS X Server 10.6
- Apple Mac OS X 10.7
- Apple Mac OS X Server 10.7
- Apple Mac OS X 10.8
- Apple Mac OS X Server 10.8

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

DESCRIPTION:

Multiple vulnerabilities have been discovered in Apple Mac OS X. The details of these vulnerabilities are as follows:

- A buffer-overflow vulnerability exists in the DirectoryService Proxy. (CVE-2012-0650)
- A buffer-overflow vulnerability occurs due to an out of bounds memory read or write error. Specifically, the issue exists in the handling of text glyphs. (CVE-2012-3716)
- A local security-bypass issue occurs in the LoginWindow component. An attacker can exploit this issue to obtain other user's login passwords. (CVE-2012-3718)
- An input validation security vulnerability exists in Mail's handling of embedded web plugins. An attacker can exploit this issue to execute web plugins when viewing a specially crafted e-mail message. (CVE-2012-3719)
- An information-disclosure vulnerability exists due to an issue in mobile accounts. Specifically, the issue occurs because creating a mobile account saves a hash of the password in the account. Attackers can exploit this issue to obtain the user's password using the hash. (CVE-2012-3720)
- A security vulnerability exists in the Device Management private interface. An attacker can exploit this issue to enumerate managed devices. (CVE-2012-3721)
- Multiple vulnerabilities in Apache, the most serious of which could lead to a denial of service. It should be noted that OS X Mountain Lion is not affected by this vulnerability. (CVE-2011-3368, CVE-2011-3607, CVE-2011-4317, CVE-2012-0021, CVE-2012-0031, CVE-2012-0053)
- Multiple vulnerabilities exist in BIND which may lead to a denial of service condition, data corruption, or information disclosure in systems configured to run BIND as a DNS nameserver. (CVE-2011-4313, CVE-2012-1667)
- Multiple memory corruption vulnerabilities exist due to the way that libpng handles PNG images. (CVE-2011-3026, CVE-2011-3048)
- An integer overflow vulnerability exists when viewing specially crafted TIFF images that could lead to arbitrary code execution. (CVE-2012-1173)
- A stack buffer overflow vulnerability exists in the handling of ICU local ID's that may allow arbitrary code execution. (CVE-2011-4599)
- A logic issue exists due to the handling of debug system calls. This vulnerability may allow a malicious program to execute code in other programs with the same user privileges. (CVE-2012-0643)
- Multiple vulnerabilities exist in PHP. The most severe vulnerability could lead to remote code execution. (CVE-2012-0831, CVE-2012-1172, CVE-2012-1823,

CVE-2012-2143, CVE-2012-2311, CVE-2012-2386, CVE-2012-2688, CVE-2011-3048)

- A memory corruption vulnerability exists due to the way QuickLook handles .pict files that could lead to remote code execution. (CVE-2012-0671)
- An integer overflow vulnerability exists in QuickTime's handling of sean atoms that could lead to remote code execution. (CVE-2012-0670)
- An uninitialized memory access vulnerability exists due to the improper handling of Sorenson encoded movie files that could lead to remote code execution. (CVE-2012-3722)
- A buffer overflow vulnerability exists due to the handling of RLE encoded movie files that could lead to remote code execution. (CVE-2012-0668)
- A memory corruption issue exists in the handling of USB hub descriptors which could allow for remote code execution. (CVE-2012-3723)

These patches also enable Ruby OpenSSL empty fragments in order to mitigate attacks on the confidentiality of SSL 3.0 and TLS 1.0 when a cypher suite uses a block cipher in CBC mode. (CVE-2011-3389)

Successful exploitation of any of these remote code execution vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed attempts could result in a denial-of-service.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply appropriate patches provided by Apple to affected 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.
- Permit local access for trusted individuals only. Where possible, use restricted environments and restricted shells.
- Remind users not to download or open files from un-trusted websites.
- Remind users not to open e-mail attachments from unknown users or suspicious e-mails from trusted sources.
- Remind users not to click links from unknown sources, or to click links without verifying the intended destination.

REFERENCES:

Apple:

<http://support.apple.com/kb/HT5501>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3368>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3607>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-4317>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0021>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0031>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0053>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-4313>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1667>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3716>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0650>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3026>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3048>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1173>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0652>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-4599>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0643>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3718>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3719>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3720>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0831>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1172>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1823>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2143>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2311>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2386>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2688>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3048>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3721>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0671>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0670>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3722>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0668>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3389>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3723>

SecurityFocus:

<http://www.securityfocus.com/bid/55623>
<http://www.securityfocus.com/bid/50802>
<http://www.securityfocus.com/bid/51705>
<http://www.securityfocus.com/bid/51407>
<http://www.securityfocus.com/bid/50690>
<http://www.securityfocus.com/bid/53772>
<http://www.securityfocus.com/bid/52830>
<http://www.securityfocus.com/bid/52891>
<http://www.securityfocus.com/bid/53457>
<http://www.securityfocus.com/bid/52364>
<http://www.securityfocus.com/bid/51954>
<http://www.securityfocus.com/bid/53403>
<http://www.securityfocus.com/bid/53388>
<http://www.securityfocus.com/bid/53729>
<http://www.securityfocus.com/bid/47545>
<http://www.securityfocus.com/bid/54638>
<http://www.securityfocus.com/bid/53579>