

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.

DATE(S) ISSUED:

2/2/2012

SUBJECT:

Multiple Vulnerabilities in Apple Mac OS X Could Allow Remote Code Execution

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 can be exploited if a user visits or is redirected to a specially crafted webpage or opens a specially crafted file, including an email attachment, using a vulnerable version of OS X. 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 OS X Lion 10.7.3 and earlier
Apple OS X Server v10.6.8

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 that could allow both remote and local code execution. These vulnerabilities can be exploited if a user visits or is redirected to a specially crafted webpage or opens a specially crafted file, including an email attachment, with a vulnerable version of Apple Mac OS X.

Apple has identified the following vulnerabilities:

A vulnerability exists in the Address Book application in Mac OS X Lion v10.7.3 or earlier. This issue exists because the application will attempt an unencrypted connection to obtain CardDAV data if an encrypted connection fails. Attackers can exploit this issue by performing a man in the middle attack or by intercepting the unencrypted data at strategic network locations. Successful exploitation could result in the theft of address book contact information. This issue affects OS X Lion v10.7 to v10.7.2, OS X Lion Server v10.7 to v10.7.2 (CVE-2011-3444)

An unspecified memory management issue exists in the Font Book application due the improper handling of certain data-font files. To exploit this issue, an attacker creates a specially crafted data-font file and distributes that file to unsuspecting users. When the user opens the file with Font Book, the exploit is triggered. Successful exploitation could result in remote code execution. This issue affects Mac OS X v10.6.8, Mac OS X Server v10.6.8, OS X Lion v10.7 to v10.7.2, OS X Lion Server v10.7 to v10.7.2. (CVE-2011-3446)

An issue exists in the CFNetwork's handling of malformed URLs which could lead to information disclosure. When accessing a maliciously crafted URL, CFNetwork could send the request to an incorrect origin server. To exploit this issue, an attacker distributes a specially crafted URL to unsuspecting users. When a user visits the URL, certain information could be relayed to the attacker. Successful exploitation could result in information disclosure which could be used to aid additional attacks. This issue affects OS X Lion v10.7 to v10.7.2, OS X Lion Server v10.7 to v10.7.2 (CVE-2011-3246)

An integer overflow vulnerability exists due to the way CFNetwork handles certain images with embedded ColorSynch information. To exploit this issue, an attacker distributes a specially crafted image file to unsuspecting users. When the file is executed, the exploit triggers. Successful exploitation could result in remote code execution. This issue affects OS X Lion v10.7 to v10.7.2, OS X Lion Server v10.7 to v10.7.2 (CVE-2011-3447) and Mac OS X v10.6.8, Mac OS X Server v10.6.8 (CVE-2011-0200)

A buffer overflow vulnerability exists in a CoreAudio component of Mac OS X v10.6.8 and Mac OS X Server v10.6.8 due to the improper handling of certain encoded audio streams. The specifics of how this vulnerability can be exploited are unclear. However, successful exploitation does involve the execution of a specially crafted audio content and could result in remote code execution. (CVE-2011-3252)

A heap buffer overflow exists in a CoreMedia component of Mac OS X due to the improper handling on H.264 encoded movie files. To exploit this issue, an attacker distributes a specially crafted movie file to unsuspecting users. When the file is executed, the exploit is triggered. Successful exploitation could result in remote code execution. This issue affects Mac OS X v10.6.8, Mac OS X Server v10.6.8, OS X Lion v10.7 to v10.7.2, OS X Lion Server v10.7 to v10.7.2. (CVE-2011-3448)

An unspecified after free issue exists in the handling of certain font files. To exploit this issue, an attacker creates and distributes a specially crafted file that uses the vulnerable fonts. When the file is execution the exploit occurs. Successful exploitation could result in remote code execution. This issue affects Mac OS X v10.6.8, Mac OS X Server v10.6.8, OS X Lion v10.7 to v10.7.2, OS X Lion Server v10.7 to v10.7.2 (CVE-2011-3449)

An unbounded stack allocation issue exists in CoreUI's handling of long URLs. To exploit this issue, an attacker creates and distributes a specially crafted website designed to leverage the issue. When a user visits the website the exploit is triggered. Successful exploitation could result in remote code execution. This issue affects OS X Lion v10.7 to v10.7.2, OS X Lion Server v10.7 to v10.7.2 (CVE-2011-3450)

An unspecified buffer overflow vulnerability exists in the "uncompress" command line tool. To exploit this issue, an attacker distributes a specially crafted compressed file. When the file is uncompressed via command line, the exploit is triggered. Successful exploitation could result in remote code execution. This issue affects Mac OS X v10.6.8, Mac OS X Server v10.6.8, OS X Lion v10.7 to v10.7.2, OS X Lion Server v10.7 to v10.7.2 (CVE-2011-0241)

A buffer overflow exists in libtiff's handling of ThunderScan encoded TIFF image files and libpng v1.5.4's handling of certain PNG files. To exploit this issue, an attacker distributes a specially crafted TIFF file or PNG file. When the file is executed, the exploit is triggered. Successful exploitation could result in code execution. This issue affects Mac OS X v10.6.8, Mac OS X Server v10.6.8, OS X Lion v10.7 to v10.7.2, OS X Lion Server v10.7 to v10.7.2 (CVE-2011-1167, CVE-2011-3328)

An unspecified issue exists in Libinfo's handling of hostname lookup requests. Libinfo could return incorrect results for a maliciously crafted hostname. To exploit this issue, an attacker creates a specially crafted website and distributes a link to unsuspecting users. When a user visits the site, the exploit is triggered. Successful exploitation could result in remote code execution. This issue affects OS X Lion v10.7 to v10.7.2, OS X Lion Server v10.7 to v10.7.2 (CVE-2011-3441)

An unspecified integer overflow exists in the parsing of certain DNS resource records. The details of how this vulnerability can be exploited are unavailable. Successful exploitation could allow remote code execution. This issue affects Mac OS X v10.6.8, Mac OS X Server v10.6.8, OS X Lion v10.7 to v10.7.2, OS X Lion Server v10.7 to v10.7.2 (CVE-2011-3453)

Multiple memory corruption issues exist in OpenGL's handling of GLSL compilation. The details of how this vulnerability can be exploited are unclear. However, successful exploitation could result in arbitrary code execution. This issue affects Mac OS X v10.6.8, Mac OS X Server v10.6.8, OS X Lion v10.7 to v10.7.2, OS X Lion Server v10.7 to v10.7.2 (CVE-2011-3457)

Multiple buffer overflow and memory corruption vulnerabilities exist in QuickTime which could allow remote code execution. To exploit these vulnerabilities, an attacker distributes a specially crafted movie or image file to unsuspecting users. When the file is executed the exploit is triggered. Successful exploitation could result in arbitrary code execution. This issue affects Mac OS X v10.6.8, Mac OS X Server v10.6.8, OS X Lion v10.7 to v10.7.2, OS X Lion Server v10.7 to v10.7.2 (CVE-2011-3458, CVE-2011-3248, CVE-2011-3459, CVE-2011-3250, CVE-2011-3460, CVE-2011-3249)

An issue exists in the Time Machine application that could allow attackers to gain unauthorized access to system backups. The user may designate a remote AFP volume or Time Capsule to be used for Time Machine backups. Time Machine did not verify that the same device was being used for subsequent backup operations. An attacker who is able to spoof the remote volume could gain access to new backups created by the user's system. This issue affects OS X Lion v10.7 to v10.7.2, OS X Lion Server v10.7 to v10.7.2. (CVE-2011-3462)

An issue exists in WebDAV Sharing's handling of user authentication. A user with a valid account on the server or one of its bound directories could cause the execution of arbitrary code with system privileges. The details of how this vulnerability can be exploited are unavailable. This issue affects OS X Lion Server v10.7 to v10.7.2 (CVE-2011-3463)

A memory corruption issue existed in FreeType's handling of Type 1 fonts. To exploit this issue, an attacker distributes a specially crafted PDF file which utilizes the vulnerable font. When a user opens the file, the exploit is triggered. Successful exploitation could result in remote code execution. This issue affects Mac OS X v10.6.8, Mac OS X Server v10.6.8, OS X Lion v10.7 to v10.7.2, OS X Lion Server v10.7 to v10.7.2 (CVE-2011-3256)

Successful exploitation of these 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:

The following actions should be taken:

- Apply appropriate patches provided by Apple to affected systems immediately after appropriate testing.
- 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.
- 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.

REFERENCES:

Apple:

<http://support.apple.com/kb/HT5130>

Security Focus:

<http://www.securityfocus.com/advisories/23952>

<http://www.securityfocus.com/bid/51807>

<http://www.securityfocus.com/bid/51808>

<http://www.securityfocus.com/bid/51809>

<http://www.securityfocus.com/bid/51810>

<http://www.securityfocus.com/bid/51811>

<http://www.securityfocus.com/bid/51812>

<http://www.securityfocus.com/bid/51813>

<http://www.securityfocus.com/bid/51814>

<http://www.securityfocus.com/bid/51815>

<http://www.securityfocus.com/bid/51816>

<http://www.securityfocus.com/bid/51817>

<http://www.securityfocus.com/bid/51818>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3444>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3446>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3246>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3447>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0200>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3252>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3448>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3449>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3459>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0241>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3328>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1167>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3441>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3453>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3457>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3249>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3460>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3250>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3459>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3248>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3458>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3462>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3463>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3256>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3450>