



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

May 23, 2013

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:

SA2013-048

DATE(S) ISSUED:

05/23/2013

SUBJECT:

Multiple Vulnerabilities in Apple QuickTime Could Allow Remote Code Execution

OVERVIEW:

Multiple vulnerabilities have been discovered in Apple QuickTime that could allow remote code execution. Apple QuickTime Player is used to play media files on Microsoft Windows and Mac OS X operating systems. 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 Apple QuickTime Player. 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 QuickTime versions prior to 7.7.4 for Windows and Mac OS X

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 remote code execution vulnerabilities have been discovered in Apple QuickTime that could allow remote 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.

The vulnerabilities are as follows:

- A memory-corruption vulnerability occurs when handling specially crafted TeXML files. [CVE-2013-1015]
- A Remote buffer-overflow vulnerability exists when handling specially crafted H.263 encoded movie files. [CVE-2013-1016]
- A Remote buffer-overflow vulnerability exists when handling specially crafted 'dref' atoms. [CVE-2013-1017]
- A Remote buffer-overflow vulnerability exists when handling specially crafted H.264 encoded movie files. [CVE-2013-1018]
- A Remote buffer-overflow vulnerability exists when handling specially crafted MP3 files. [CVE-2013-0989]
- A Remote buffer-overflow vulnerability exists when handling specially crafted Sorenson encoded movie files. [CVE-2013-1019]
- A memory-corruption vulnerability occurs when handling specially crafted JPEG encoded data. [CVE-2013-1020]
- A memory-corruption vulnerability occurs when handling specially crafted QTIF files. [CVE-2013-0987]
- A Remote buffer-overflow vulnerability exists when handling specially crafted JPEG encoded data of malicious movie files. [CVE-2013-1021]
- A Remote buffer-overflow vulnerability exists when handling specially crafted 'enof' atoms of malicious movie files. [CVE-2013-0986]
- A Remote buffer-overflow vulnerability exists when handling specially crafted FPX files. [CVE-2013-0988]
- A Remote buffer-overflow vulnerability exists when handling specially crafted 'mvhd' atoms of malicious movie files. [CVE-2013-1022]

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.

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.
- 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/HT5770>

Security Focus:

<http://www.securityfocus.com/advisories/28279>

<http://www.securityfocus.com/bid/60086>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1015>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1016>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1017>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1018>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1019>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1020>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1021>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1022>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0986>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0987>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0988>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0989>