



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

August 21, 2015

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:
SA2015-103**

**DATE(S) ISSUED:
08/21/2015**

**SUBJECT:
Multiple Vulnerabilities in Apple QuickTime Could Allow Remote Code Execution**

OVERVIEW:
Multiple vulnerabilities have been discovered in Apple QuickTime. QuickTime is a multimedia application that is capable of playing video, sound, and image files. These vulnerabilities can be exploited if a user opens a specially crafted file, including an email attachment. Successful exploitation could result in unexpected application crashes and remote code execution within the context of the application. 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.

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

SYSTEM AFFECTED:
• Apple QuickTime 7 Prior To 7.7.8 for Microsoft Windows 7 and Windows Vista

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

TECHNICAL SUMMARY:

Multiple memory-corruption vulnerabilities have been discovered in Apple QuickTime 7 that could allow for remote code execution. These vulnerabilities can be exploited if a user

opens a specially crafted file, including an email attachment. (CVE-2015-3772, CVE-2015-3779, CVE-2015-5753, CVE-2015-5779, CVE-2015-3765, CVE-2015-3788, CVE-2015-3789, CVE-2015-3790, CVE-2015-3791, CVE-2015-3792, CVE-2015-5751), CVE-2015-5785, CVE-2015-5786)

Successful exploitation could result in unexpected application crashes and remote code execution within the context of the application. 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 updates provided by Apple to vulnerable 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, accept, or execute files from un-trusted or unknown sources.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

REFERENCES:

Apple:

<https://support.apple.com/en-us/HT205046>

US-CERT:

<https://www.us-cert.gov/ncas/current-activity/2015/08/20/Apple-Releases-Security-Update-QuickTime>