

*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.*

**TLP: WHITE**

**Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.**

<http://www.us-cert.gov/tlp/>

**DATE(S) ISSUED:**

01/08/2016

**SUBJECT:**

Multiple Vulnerabilities in Apple QuickTime Could Allow Arbitrary Code Execution

**OVERVIEW:**

Multiple vulnerabilities have been discovered in Apple QuickTime, which could allow an attacker to potentially execute arbitrary code. 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 arbitrary code execution within the context of the application. Depending on the privileges associated with the application, 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 7.7.9 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 arbitrary code execution. These vulnerabilities can be exploited if a user opens a specially crafted movie file, including an email attachment. The memory corruption issues were addressed through improved memory handling in QuickTime 7.7.9. (CVE-2015-7085, CVE-2015-7086, CVE-2015-7087, CVE-2015-7088, CVE-2015-7089, CVE-2015-7090, CVE-2015-7091, CVE-2015-7092, CVE-2015-7117)

Successful exploitation could result in unexpected application crashes and arbitrary code execution within the context of the application. Depending on the privileges associated with the application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

#### **RECOMMENDATIONS:**

The following actions should 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/HT205638>

##### **CVE:**

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7085>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7086>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7087>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7088>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7089>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7090>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7091>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7092>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7117>

**TLP: WHITE**

**Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.**

<http://www.us-cert.gov/tlp/>