

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:

04/23/2014

SUBJECT:

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

EXECUTIVE SUMMARY:

Multiple vulnerabilities have been discovered in Apple's Mac OS X, Mac OS X Server, and Apple Safari that could allow remote code execution. Mac OS X and Mac OS X Server are operating systems for Apple computers. Apple Safari is a web browser available for Mac OS X and Microsoft Windows. 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 or Apple Safari. 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.

THREAT INTELLIGENCE

At this time there is no known proof-of-concept code available.

SYSTEM AFFECTED:

- Apple Mac OS X 10.7.5
- Apple Mac OS X 10.8.5
- Apple Mac OS X 10.9.2
- Apple Mac OS X Server 10.7.5
- Apple Safari 6.1.2 and Safari 7.0.2 and earlier

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 vulnerabilities have been discovered in Apple's Mac OS X, Mac OS X Server, and Apple Safari. These vulnerabilities can be exploited if a user visits or is redirected to a specially crafted webpage or opens a specially crafted file. Details of these vulnerabilities are as follows:

- A security bypass vulnerability affects the 'Secure Transport' component. Specially, this issue occurs in the handling of SSL renegotiations. This issue does not affect Mac OS X 10.7 systems and earlier. [CVE-2014-1295]
- A security bypass vulnerability affects the 'CFNetwork HTTPProtocol' component. This issue exists in the handling of incomplete HTTP header lines. [CVE-2014-1296]
- A remote arbitrary code-execution vulnerability affects the 'CoreServicesUIAgent' component. Specifically, this issue exists in the handling of the formatting of URLs. This issue does not affect systems prior to OS X 10.9. [CVE-2014-1315]
- A buffer underflow exists in the 'FontParser' component. Specifically, this issue exists in the handling of fonts in PDF files. This issue does not affect OS X 10.9 systems. [CVE-2013-5170]
- A remote denial of service vulnerability exists in the 'Heimdal Kerberos' component. Specifically, this issue exists in the handling of ASN.1 data. [CVE-2014-1316]
- A buffer overflow vulnerability exists in the 'ImageIO' component. Specifically, this issue exists in the handling of JPEG images. This issue does not affect systems prior to OS X 10.9. [CVE-2014-1319]
- A remote security-bypass vulnerability exists in the 'Intel Graphics Driver' component. Specifically, this issue exists due to improper validation when handling a pointer from userspace. [CVE-2014-1318]
- A kernel address space layout randomization bypass vulnerability exists in the 'IOKit Kernel' component. Specifically, this issue exists due to the reading of kernel pointers by local users. [CVE-2014-1320]
- A kernel address space layout randomization bypass vulnerability exists in the 'Kernel' component. Specifically, this issue exists due to the reading of kernel pointers by local users. [CVE-2014-1322]
- A local security-bypass vulnerability exists in the 'Power Management' component. Specifically, this issue occurs in the handling keypresses while going to sleep. This issue does not affect systems prior to OS X 10.9. [CVE-2014-1321]
- An integer overflow vulnerability exists in the 'Ruby' component. Specifically, this issue occurs in the handling of YAML tags. This issue does not affect systems prior to OS X 10.9. [CVE-2013-6393]
- A heap-based buffer overflow vulnerability affects the 'Ruby' component. Specially, this issue occurs in the conversion of a string to a floating-point value. [CVE-2013-4164]
- A remote arbitrary code-execution vulnerability affects the 'WindowServer' component. Specifically, this issue occurs because the component allows for the creation of WindowServer sessions for sandboxed applications. [CVE-2014-1314]
- Multiple memory corruption vulnerabilities exist in Safari.
- An arbitrary file disclosure vulnerability exists in Safari. This issue occurs in the handling of IPC messages from the WebProcess component of Safari.

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:

The following actions should 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, unknown users, or suspicious emails.
- 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/HT6207>

Security Focus:

<http://www.securityfocus.com/bid/63873>

<http://www.securityfocus.com/bid/66242>

<http://www.securityfocus.com/bid/67021>

<http://www.securityfocus.com/bid/67022>

<http://www.securityfocus.com/bid/67023>

<http://www.securityfocus.com/bid/67025>

<http://www.securityfocus.com/bid/67026>

<http://www.securityfocus.com/bid/67028>

<http://www.securityfocus.com/bid/67029>

<http://www.securityfocus.com/bid/67030>

<http://www.securityfocus.com/bid/66242>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1296>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1315>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5170>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1316>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1319>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1318>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1320>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1322>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1321>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-6393>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-4164>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1295>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1314>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2871>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2926>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2928>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-6625>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1289>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1290>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1291>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1292>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1293>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1294>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1298>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1299>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1300>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1301>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1302>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1303>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1304>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1305>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1307>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1308>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1309>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1310>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1311>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1312>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1313>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1713>