

*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:**

12/4/2014

**SUBJECT:**

Multiple Vulnerabilities in WebKit Could Allow for Remote Code Execution

**EXECUTIVE SUMMARY:**

Multiple vulnerabilities have been discovered in the WebKit browser engine, which is used primarily to power the Apple Safari browser. Successful exploitation of these vulnerabilities could result in remote code execution; potentially allowing for an attacker to gain control of a host and have the same privileges as the user running the affected 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 is no known proof-of-concept code available at this time.

**SYSTEM AFFECTED:**

- Apple Safari prior to 6.2.1

**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 exist in WebKit that could allow remote code execution. These issues were addressed through improved memory handling.

WebKit is an open source browser engine that is used by multiple applications, and is used to power the Apple Safari web browser. In addition to Safari, older versions of the Google Chrome browser, prior to version 27, also use WebKit.

The vulnerabilities can be exploited if a user visits, or is redirected to, a specially crafted web page. Successful exploitation of these vulnerabilities could result in remote code execution; potentially allowing for an attacker to gain control of a host and have the same privileges as the user running the affected 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.

Currently no working exploits have been reported, and Apple has released updates to resolve the issues for their Safari browser.

## **RECOMMENDATIONS:**

The following actions should be taken:

- Update vulnerable products 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 visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Do not open email attachments or click on URLs from unknown or un-trusted sources.

## **REFERENCES:**

### **Apple:**

<http://support.apple.com/en-us/HT6596>

### **CVE:**

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1748>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4452>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4459>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4465>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4466>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4468>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4469>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4470>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4471>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4472>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4473>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4474>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4475>

**Security Focus:**

<http://www.securityfocus.com/bid/71464>

<http://www.securityfocus.com/bid/71451>