

*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:**

09/10/2013

**SUBJECT:**

Multiple Vulnerabilities in Adobe Flash Player Could Allow Remote Code Execution (APSB13-21)

**OVERVIEW:**

Multiple vulnerabilities have been discovered in Adobe Flash Player that could allow an attacker to take control of the affected system. Adobe Flash Player is a widely distributed multimedia and application player used to enhance the user experience when visiting web pages or reading email messages. 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. Failed exploit attempts will likely cause denial-of-service conditions.

**SYSTEM AFFECTED:**

- Adobe Flash Player 11.8.800.94 and earlier versions for Windows and Macintosh
- Adobe Flash Player 11.2.202.297 and earlier versions for Linux
- Adobe Flash Player 11.1.115.69 and earlier versions for Android 4.x
- Adobe Flash Player 11.1.111.64 and earlier versions for Android 3.x and 2.x
- Adobe AIR 3.8.0.870 and earlier versions for Windows and Android
- Adobe AIR 3.8.0.910 and earlier versions for Macintosh
- Adobe AIR 3.8.0.870 SDK & Compiler and earlier versions for Windows
- Adobe AIR 3.8.0.910 SDK & Compiler and earlier versions for Macintosh

**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:**

Adobe Flash Player is prone to multiple vulnerabilities that could allow for remote code execution. Specifically, the vulnerabilities identified may allow an attacker to corrupt the application's memory in such a way that results in remote code execution. Failed exploitation attempts may cause denial-of-service conditions. 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. Failed exploit attempts will likely cause denial-of-service conditions.

## **RECOMMENDATIONS:**

The following actions should be taken:

- Install the updates provided by Adobe immediately after appropriate testing.
- Users of Adobe Flash Player 11.8.800.94 and earlier versions for Windows and Macintosh should update to Adobe Flash Player 11.8.800.168.
- Users of Adobe Flash Player 11.2.202.297 and earlier versions for Linux should update to Adobe Flash Player 11.2.202.310.
- Adobe Flash Player 11.8.800.97 installed with Google Chrome will automatically be updated to the latest Google Chrome version, which will include Adobe Flash Player 11.8.800.170 for Windows, Macintosh and Linux.
- Adobe Flash Player 11.8.800.94 installed with Internet Explorer 10 will automatically be updated to the latest Internet Explorer 10 version, which will include Adobe Flash Player 11.8.800.168 for Windows 8.
- Users of Adobe Flash Player 11.1.115.69 and earlier versions on Android 4.x devices should update to Adobe Flash Player 11.1.115.81.
- Users of Adobe Flash Player 11.1.111.64 and earlier versions for Android 3.x and 2.x should update to Flash Player 11.1.111.73.
- Users of Adobe AIR 3.8.0.870 and earlier versions for Windows and Android should update to Adobe AIR 3.8.0.1430.
- Users of Adobe AIR 3.8.0.910 and earlier versions for Macintosh should update to Adobe AIR 3.8.0.1430.
- Users of the Adobe AIR 3.8.0.870 SDK & Compiler and earlier versions for Windows should update to the Adobe AIR 3.8.0.1430 SDK & Compiler.
- Users of the Adobe AIR 3.8.0.910 SDK & Compiler and earlier versions for Macintosh should update to the Adobe AIR 3.8.0.1430 SDK & Compiler.
- 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 untrusted websites or follow links provided by unknown or untrusted sources.
- Do not open email attachments from unknown or untrusted sources.

## **REFERENCES:**

### **Adobe:**

<https://www.adobe.com/support/security/bulletins/apsb13-21.html>

### **CVE:**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3361>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3362>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3363>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5324>

**SecurityFocus:**

<http://www.securityfocus.com/bid/62290>

<http://www.securityfocus.com/bid/62294>

<http://www.securityfocus.com/bid/62295>

<http://www.securityfocus.com/bid/62296>