

# ISSO Information Alert

2/14/2012

## Adobe Shockwave Player

### MULTI-STATE INFORMATION SHARING AND ANALYSIS CENTER CYBER SECURITY ADVISORY

**MS-ISAC ADVISORY NUMBER:**

2012-007

**DATE(S) ISSUED:**

2/14/2012

**SUBJECT:**

Multiple Vulnerabilities in Adobe Shockwave Player Could Allow For Remote Code Execution

**OVERVIEW:**

Multiple vulnerabilities have been discovered in Adobe Shockwave, which could allow an attacker to take complete control of an affected system. Adobe Shockwave is a multimedia platform used to add animation and interactivity to web pages. These vulnerabilities may be exploited if a user visits or is redirected to a specially crafted web page or when a user opens a specially crafted file. 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.

**SYSTEMS AFFECTED:**

- Adobe Shockwave Player (versions prior to 11.6.4.634)

**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 Shockwave Player is prone to multiple memory corruption vulnerabilities that could allow for remote code execution. Details of these vulnerabilities are as follows:

- Seven memory corruption vulnerabilities exist in the Shockwave 3D Asset that could lead to remote code execution.
- A heap overflow vulnerability exists that could lead to remote code execution.
- An unspecified memory corruption vulnerability exists that could lead to remote code execution.

Successful exploitation of any of these vulnerabilities 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:**

We recommend the following actions be taken:

- Install the 11.6.4.634 update from Adobe immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Do not open email attachments or follow web links from unknown or untrusted sources.
- Consider implementing file extension white lists for allowed e-mail attachments.

#### **REFERENCES:**

##### **Adobe:**

<http://www.adobe.com/support/security/bulletins/apsb12-02.html>

##### **CVE:**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0757>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0758>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0759>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0760>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0761>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0762>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0763>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0764>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0766>