



**State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory**

August 10, 2011

The following cyber advisory was issued by the State of Alaska and was 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.

ADVISORY NUMBER:

SA2011-048

DATE(S) ISSUED:

08/10/2011

SUBJECT:

Multiple Vulnerabilities in Adobe Shockwave Player Could Allow For Remote Code Execution (APSB11-19)

OVERVIEW:

Multiple memory corruption 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 will 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:

- Shockwave Player 11.6.0.626 and earlier versions for Windows and 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 Shockwave Player is prone to multiple memory corruption vulnerabilities that could allow for remote code execution. Details of these vulnerabilities are as follows:

- A memory corruption vulnerability exists in the 'IML32.dll' library component that could lead to remote code execution.
- A memory corruption vulnerability occurs when Shockwave Player parses a '.dir' media file in the 'Dirapi.dll' library component that could lead to remote code execution.
- A memory corruption vulnerability exists in the 'Textra.x32' component that could lead to remote code execution.
- A memory corruption vulnerability exists in the 'msvcr90.dll' library component that could lead to remote code execution.
- Multiple unspecified memory corruption vulnerabilities could lead to remote code execution.

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 crash the affected application.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Install the 11.6.1.629 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/apsb11-19.html>

Security Focus:

<http://www.securityfocus.com/bid/49102>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2419>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2421>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2422>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2423>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4308>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4309>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2420>