



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

December 18, 2012

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:

SA2012-083

DATE(S) ISSUED:

12/18/2012

SUBJECT:

Adobe Shockwave Player Remote Code Execution Vulnerability

OVERVIEW:

A vulnerability has been discovered in Adobe Shockwave, which could allow for remote code execution. Adobe Shockwave is a multimedia platform used to add animation and interactivity to web pages. This vulnerability may be exploited if a user visits, or is redirected to, a specially crafted web page. It may also be exploited 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.

SYSTEMS AFFECTED:

- Adobe Shockwave Player (Versions 11.6.8.638 and earlier) 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 a remote code-execution vulnerability because of an error in the Flash runtime. Specifically, this issue occurs in the 'Flash Asset.x32' file. Attackers can exploit this issue to execute arbitrary code in the context of the affected application. Failed exploit attempts will likely result in 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.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Disable the Shockwave Player ActiveX control in Internet Explorer by setting the kill bit for the following CLSIDs:
 - o {166B1BCA-3F9C-11CF-8075-444553540000}
 - o {233C1507-6A77-46A4-9443-F871F945D258}
- More information about how to set the kill bit is available in Microsoft Support Document 240797, which can be found at <http://support.microsoft.com/kb/240797>.
- Alternatively, the following text can be saved as a .REG file using Windows Registry Editor Version 5.00 and imported to set the kill bit for this control:
 - o [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\InternetExplorer\ActiveX Compatibility\{166B1BCA-3F9C-11CF-8075-444553540000} "Compatibility Flags"=dword:00000400
 - o [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\ActiveX Compatibility\{166B1BCA-3F9C-11CF-8075-444553540000} "Compatibility Flags"=dword:00000400
 - o [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\InternetExplorer\ActiveX Compatibility\{233C1507-6A77-46A4-9443-F871F945D258}] "Compatibility Flags"=dword:00000400
 - o [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\ActiveX Compatibility\{233C1507-6A77-46A4-9443-F871F945D258}] "Compatibility Flags"=dword:00000400
- 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.
- Inform and educate users regarding the threats posed by attachments and hypertext links contained in emails especially from un-trusted sources.
- Consider implementing file extension white lists for allowed e-mail attachments.

REFERENCES:

SecurityFocus:

<http://www.securityfocus.com/bid/56973>

US CERT:

<http://www.kb.cert.org/vuls/id/323161>