

State of Alaska State Security Office



State of Alaska Cyber Security & Critical Infrastructure Cyber Advisory

October 20, 2010

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:
SA2010-080

DATE(S) ISSUED:
10/21/2010
10/28/2010 - **Updated**

SUBJECT:
Vulnerability in Adobe Shockwave Player Could Allow Remote Code Execution

ORIGINAL OVERVIEW:
A vulnerability has been discovered in Adobe Shockwave Player that could allow remote code execution. Adobe Shockwave Player is a widely used multimedia application used to display animations and video when visiting web sites. This vulnerability can be exploited by visiting a web page that contains a malicious Adobe Shockwave file. Successful exploitation may result in an attacker gaining the same privileges as the logged on user within the scope of the 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. Failed exploitation could result in denial-of-service conditions.

Please note that there is no patch available for this vulnerability. Exploit code is publicly available but we have not received any reports of active exploitation.

October 28 – UPDATED OVERVIEW

Adobe has released an update that resolves this vulnerability in addition to several other vulnerabilities. Adobe also reports that this vulnerability is being exploited on the Internet.

SYSTEMS AFFECTED:

- All versions prior to and including Adobe Shockwave Player 11.5.8.612

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

ORIGINAL DESCRIPTION:

A vulnerability has been discovered in Adobe Shockwave Player that could allow for remote code execution because it fails to properly parse 'rcsL' chunks of the Director's RIFF-based file format. This could all allow an attacker to change the value of the EAX register in order to control the pointer responsible for calculating an offset into a heap-based buffer. This vulnerability can be exploited if a user visits a specially crafted web page designed to exploit this vulnerability. Successful exploitation may result in an attacker gaining the same privileges as the logged on user within the scope of the 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. Failed exploitation could result in denial-of-service conditions.

~~Please note that there is no patch available for this vulnerability. Exploit code is publicly available but we have not received any reports of active exploitation.~~

October 28 – UPDATED DESCRIPTION

Adobe has released an update that resolves this vulnerability in addition to several other vulnerabilities. Adobe also reports that this vulnerability is being exploited on the Internet.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply appropriate patches provided by Adobe to vulnerable systems as soon as they become available.
- 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.

October 28 – UPDATED RECOMMENDATIONS

We recommend the following actions be taken:

- *Apply appropriate updates provided by Adobe to vulnerable systems immediately after appropriate testing.*

ORIGINAL REFERENCES:

Security Focus:

<http://www.securityfocus.com/bid/44291>

October 28 – UPDATED REFERENCES

Adobe:

<http://www.adobe.com/support/security/advisories/apsa10-04.html>

<http://www.adobe.com/support/security/bulletins/apsb10-25.html>

<http://blogs.adobe.com/psirt/>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3653>