



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

**January 4, 2007**

*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.*

**STATE OF ALASKA ADVISORY NUMBER:**

2008-001

**DATE ISSUED:**

January 4, 2008

**SUBJECT:**

Shockwave Flash (SWF) files may contain cross-site scripting vulnerabilities

**OVERVIEW:**

Many websites employ 3D animation or movies using Shockwave Flash (SWF) files to enhance the user experience when visiting web sites. If your website is hosting a SWF file, it may be used by attackers to exploit users visiting the website, giving the attacker complete control over the user's session. A book, *Hacking Exposed: Web 2.0, Web 2.0 Security Secrets and Solutions*, detailing these vulnerabilities was recently published.

**SYSTEMS AFFECTED:**

Rich Cannings, a security researcher and author, recently released a document identifying various web authoring tools that can produce vulnerable SWF files such as:

- Adobe Dreamweaver
- Adobe Acrobat Connect, formerly Macromedia Breeze
- Infsoft FusionCharts
- Techsmith Camtasia

Additionally, he notes that any software product that can save or export SWF file formats may also produce vulnerable SWF files.

**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: N/A****DESCRIPTION:**

The vulnerabilities are related to web authoring tools used to generate Flash content and other tools that can save or export SWF files. Any website hosting Flash files generated by an affected product is vulnerable to cross-site scripting in the context of the domain hosting the vulnerable file.

ActionScript is a scripting language used primarily for the development of websites and software using Adobe Flash. The resulting Flash content is typically published in the form of SWF files embedded in web pages. ActionScript within a Flash file creates dynamic content on the web and interacts with web browsers in a manner similar to JavaScript, VBScript, and other client-side scripting languages. As with traditional script content in HTML pages, improperly validated user-controlled input in Flash files can execute arbitrary ActionScript and JavaScript in the context of the domains hosting the affected Flash files. Specifically, ActionScript specifies a special protocol for URLs in HTML text fields, asfunction, which causes a link to invoke an ActionScript function in a Flash file instead of opening a URL. An attacker could call all public and static functions by supplying a string parameter to asfunction.

Applications that generate Flash files (e.g., "save as SWF", "export to SWF", etc.) using vulnerable templates may automatically insert generic and vulnerable ActionScript into saved files. As a result, all Flash files generated by these affected applications contain cross-site scripting vulnerabilities in the domains hosting these files. Furthermore, exploitation of these vulnerabilities would be consistent across all sites using a particular product and vulnerable sites could be identified through a web search.

**RECOMMENDATIONS:**

We recommend the following actions be taken:

- Check websites for any SWF files.
- Run SWFINtruder against all SWF files (<http://code.google.com/p/swfintruder/>) and mediate any problems identified.
- Run a Flash validator against all SWF files (<http://code.google.com/p/flash-validators/>) and mediate any problems identified.
- Apply appropriate patches as they become available

- Consider removing any vulnerable SWF files that can not be remediated.
- Follow the guidelines of the Adobe whitepaper [Creating More Secure SWF Web Applications](#).
- Review the security resources available at <http://www.adobe.com/devnet/flashplayer/security.html>

#### **ACKNOWLEDGEMENTS:**

A special thanks to US-CERT for sharing their research and the content contained in this advisory.

#### **REFERENCES:**

##### **US-CERT:**

<http://www.kb.cert.org/vuls/id/945060>

<http://www.kb.cert.org/vuls/id/758769>

##### **Adobe:**

<http://www.adobe.com/support/security/advisories/apsa07-06.html>

<http://www.adobe.com/support/security/bulletins/apsb07-20.html>

##### **Adobe Secure SWF Recommendations:**

[http://www.adobe.com/devnet/flashplayer/articles/fplayer9\\_security.html](http://www.adobe.com/devnet/flashplayer/articles/fplayer9_security.html)

[http://www.adobe.com/devnet/flashplayer/articles/secure\\_swf\\_apps.html](http://www.adobe.com/devnet/flashplayer/articles/secure_swf_apps.html)

##### **Rich Cannings, Security Researcher:**

[http://docs.google.com/View?docid=ajfxntc4dmsq\\_14dt57ssdw](http://docs.google.com/View?docid=ajfxntc4dmsq_14dt57ssdw)

##### **SWFIntruder:**

<http://code.google.com/p/swfintruder/>

<https://www.owasp.org/index.php/Category:SWFIntruder>

##### **Flash Validators:**

<http://code.google.com/p/flash-validators/>