



eSecurity Advisory
Adobe Acrobat Reader Plug-in Vulnerability
(JANUARY 11 UPDATED INFORMATION)

A vulnerability has been found in multiple versions of the Adobe Acrobat Reader Plug-in, which allows users to view Portable Document Format (PDF) files via a web browser such as Internet Explorer or Firefox. **The Adobe Acrobat Reader installs the plug-in by default.**

Please note that only Adobe Acrobat Reader Plug-in is vulnerable to this attack. This vulnerability can be exploited if an attacker can convince a user to click on a maliciously crafted link (URL) to open a PDF file. The vulnerability does not exist in the PDF document but in the parameters passed to the plug-in. An attacker may be able to use this vulnerability to steal sensitive information from a user's computer or force the user's computer to visit arbitrary Web sites.

What can you do?

- **Upgrade Adobe Reader to version 8.0.0 as soon as possible. The latest version can be found at: <http://www.adobe.com/products/reader/>.**
- **For users that do not want to upgrade to Acrobat 8.0.0 at this time, we recommend that the appropriate patch be installed after appropriate testing. Patches and updated versions are available at http://www.adobe.com/products/acrobat/readstep2_allversions.html.**

Listed below is more information that may helpful to users to protect their work and home computers.

SUBJECT:

Adobe Acrobat Reader Plug-in is Prone to Cross-Site Scripting Attacks

SYSTEMS AFFECTED:

- Adobe Acrobat Reader 6.0.1
- Adobe Acrobat Reader 6.0.2
- Adobe Acrobat Reader 6.0.3
- Adobe Acrobat Reader 6.0.4
- Adobe Acrobat Reader 7.0.0
- Adobe Acrobat Reader 7.0.1
- Adobe Acrobat Reader 7.0.2
- Adobe Acrobat Reader 7.0.3
- Adobe Acrobat Reader 7.0.4
- Adobe Acrobat Reader 7.0.5
- Adobe Acrobat Reader 7.0.6
- Adobe Acrobat Reader 7.0.7
- Adobe Acrobat Standard, Professional and Elements 7.0.8 and earlier

eSecurity Advisory: Adobe Acrobat Reader Plug-in Vulnerability

Delaware Department of Technology and Information

January 12, 2007

- Adobe Acrobat 3D

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 Reader Plug-in is prone to a cross-site scripting (XSS) vulnerability because it fails to properly sanitize user input. Cross-site scripting is a vulnerability found in Web applications that unintentionally allow for code injection into the Web pages being viewed by other users. Attackers can inject JavaScript, VBScript, ActiveX, HTML, or Flash into a vulnerable application and force this code to execute on a user's machine. The results of a successful XSS attacks include the execution code on a user's computer, forcing the user's computer to visit arbitrary Web sites, and theft of cookie data. Stealing cookie data may permit the attacker to impersonate the user and hijack Web applications that use cookies for session management.

The Adobe Reader plug-in has a feature called "Open Parameters" that may be used through a URI to specify certain parameters when viewing a PDF. These parameters are not properly sanitized for malicious content. An attacker can craft malicious URI parameters to allow for the execution of arbitrary JavaScript in vulnerable web browsers in the context of a site hosting a PDF file. As a result, an attacker might be able to use the PDF vulnerability to steal cookie based authentication credentials or exploit other client-side vulnerabilities.

Based on information provided by Adobe and other vendors, Adobe's Acrobat Reader version 8.0.0, and Internet Explorer running Windows XP SP 2 with Acrobat Reader 5.0 or higher are not affected by this vulnerability. CSCIC has tested these configurations and confirmed this information.

Proof of concept code has been made available to the public.

REFERENCES:

Adobe:

<http://www.adobe.com/support/security/advisories/apsa07-01.html>

US-CERT:

<http://www.kb.cert.org/vuls/id/815960>

Symantec Security Response:

http://www.symantec.com/enterprise/security_response/weblog/2007/01/when_pdfs_attack.html

Secunia:

<http://secunia.com/advisories/23483/>

eSecurity Advisory: Adobe Acrobat Reader Plug-in Vulnerability

Delaware Department of Technology and Information

January 12, 2007

CNET:

http://news.com.com/Acrobat+flaw+could+spawn+Web+attacks/2100-1002_3-6147038.html

Websense:

<http://www.websense.com/securitylabs/alerts/alert.php?AlertID=719>

JANUARY 11 UPDATED REFERENCES

<http://www.adobe.com/support/security/bulletins/apsb07-01.html>

http://www.adobe.com/products/acrobat/readstep2_allversions.html

MS-ISAC ADVISORY NUMBER:

2007-001 – UPDATED

MS-ISAC

30 South Pearl Street, Suite P2

Albany, NY 12207