

[NEWS] Adobe SVG Viewer Active Scripting Bypass

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-10/0025.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 10/08/03

To: list@securiteam.com

Date: 8 Oct 2003 10:26:31 +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>

Adobe SVG Viewer Active Scripting Bypass

SUMMARY

Scalable Vector Graphics (SVG) is a relatively new XML-based language for creating and controlling vector graphics. The language was standardized and endorsed by the WWW Consortium (W3C).

Several SVG parsers and renderers have been released as browser plugins, but the most popular of them all is Adobe SVG Viewer (ASV). According to Adobe: "Adobe SVG Viewer 3.0 is available in 15 languages and many millions of viewers have already been distributed worldwide."

A vulnerability in the Adobe SVG allows remote attackers to cause the viewer to execute Active Scripting even though it has been specifically disabled.

DETAILS

Affected applications:

- * Adobe SVG Viewer (ASV) 3.0 and prior
- * Adobe SVG Viewer 3 Build 76

Securiteam: [NEWS] Adobe SVG Viewer Active Scripting Bypass

Note that any other application that embeds ASV is affected as well, including the WebBrowser control. Therefore, any application that makes use of the WebBrowser control is vulnerable (Internet Explorer, AOL Browser, MSN Explorer, etc.).

Technical details:

SVG documents may be manipulated by script, through a full Document Object Model that the plugin exposes. In order to achieve an independent method of manipulation, ASV creates an instance of the Microsoft JScript engine, which is then used to parse and execute scripts blocks that appear in the document.

When parsed in the browser environment, SVG documents are able to interact with the containing HTML document by using the "parent" property. By referring to the HTML document, script running in the SVG document is able to fully control the parent's content.

The problem is that ASV completely disregards the browser's Active Scripting settings. Thereby, making it easy for attackers to utilize scripting abilities and HTML DOM manipulations without having to rely on Active Scripting being enabled by the user.

Many users choose to disable Active Scripting in the browser for security reasons, since even though Active Scripting isn't in itself a threat (in most cases), it happens to be a major component in browser-based attacks.

Demonstration:

GreyMagic put together a <http://security.greymagic.com/adv/gm002-mc/script.asp> proof of concept demonstration (ASV 3.0 or prior required). Turn Active Scripting off before trying it, in order to properly test it.

Solution:

GreyMagic brought this issue to Adobe on 21-Aug-2003. They have devised a patched version (ASV 3.01) and made it available on the official ASV download site.

ADDITIONAL INFORMATION

The original advisory can be found at:

<http://security.greymagic.com/adv/gm002-mc/>
<http://security.greymagic.com/adv/gm002-mc/>.

The information has been provided by <mailto:security@greymagic.com>
GreyMagic Software.

=====

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@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

Securiteam: [NEWS] Adobe SVG Viewer Active Scripting Bypass

=====
=====

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.