

[NT] Adobe ActiveX Allows Local File Discovery

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-04/0140.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 04/25/05

To: list@securiteam.com

Date: 25 Apr 2005 15:16:33 +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 ActiveX Allows Local File Discovery

SUMMARY

A vulnerability within the Adobe Reader and Acrobat web control has been identified. Under certain circumstances, if the Internet Explorer ActiveX control is directly invoked by a web page, it is possible to discover the existence of local files by monitoring the behavior of certain methods.

DETAILS

Adobe Reader contains a Safe for Scripting method with the definition of VARIANT_BOOL LoadFile([in] BSTR fileName). A malicious user can take advantage of this if they can get their victim to navigate to their malicious website. On the website, the attacker can call the LoadFile method, passing in a local file name on their victim's computer. Using this method, the attacker is able to determine file existence on their victim's machine. Through this method it is not possible to extract the content of the file.

This attack would be useful as a stepping stone to further attacks. Knowing the existence of a local file an attacker can gain knowledge as to the software and likely versions of software the individual is using.

NOTE: This bug was discovered by NISCC in parallel prior to the fix

Securiteam: [NT] Adobe ActiveX Allows Local File Discovery

release.

Fix Information:

Upgrade info and further details from Adobe can be found here:

<<http://www.adobe.com/support/techdocs/331465.html>>

<http://www.adobe.com/support/techdocs/331465.html>. This fix was originally posted on 4/1/05.

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0035>>

CAN-2005-0035

ADDITIONAL INFORMATION

The information has been provided by <<mailto:robfly@hyperdose.com>>

Hyperdose Security.

The original article can be found at:

<<http://www.hyperdose.com/advisories/H2005-06.txt>>

<http://www.hyperdose.com/advisories/H2005-06.txt>

=====

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

=====

=====

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.