

[NEWS] Directory Traversal in Wolfram Research's webMathematica

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-06/0065.html>

From: support@securiteam.com

Date: 06/17/02

From: support@securiteam.com

To: list@securiteam.com

Date: Mon, 17 Jun 2002 21:18:26 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

Directory Traversal in Wolfram Research's webMathematica

SUMMARY

There is a vulnerability in the webMathematica software which allows remote clients (web surfers) to read an arbitrary file on the server (assuming the httpd-user has permission). This can reveal sensitive information such as that stored in /etc/passwd, /etc/inetd.conf, system logs, etc. (These examples are on UNIX -- note that Windows servers are also vulnerable.)

DETAILS

<<http://www.wolfram.com/>> webMathematica is the clear choice for adding interactive calculations to the web. This unique technology enables you to create web sites that allow users to compute and visualize results directly from a web browser.

Based on the world's leading technical computing software and the proven Java Servlet technology, webMathematica is fully compatible with Mathematica and state-of-the-art dynamic web systems.

webMathematica generates images based on user input, often involving mathematical figures or signs which cannot be displayed using normal

Securiteam: [NEWS] Directory Traversal in Wolfram Research's webMathematica

ascii-text. Generated images are named a long numeric string (randomly generated?) and are displayed in the page presented to the user. The ID of the image is passed to a cgi-script as an argument the URL, as shown below, and altering this ID can trick the script into displaying other files on the system.

Exploit:

Example normal URL:

http://www.domain.com/webMathematica/MSP?MSPStoreID=MSPStore888808189_2408042780ge/gif

Example exploited URL:

<http://www.domain.com/webMathematica/MSP?MSPStoreID=../../../../etc/passwdge/gif>

Note that the normal user would never see the above 'normal' URL, as the URL only refers the generated image. It is found by viewing the page source, or through browser-specific methods. In Internet Explorer, for example, one would right-click on the generated image and click 'Properties'.

Workaround:

Directly reference the generated image, thereby avoiding use of the 'MSP' script.

Solution:

Upgrade to the latest version of the product.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:andrewbadr@hotmail.com>>
Andrew Badr.

=====

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.

-
- **Previous message:** support@securiteam.com: "[NT] Console Java Applications can Leak Passphrases on Windows"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)