

[NEWS] Cross Site Scripting in Mozilla Firefox

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-03/0076.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 03/17/05

To: list@securiteam.com

Date: 17 Mar 2005 10:29:54 +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>

Cross Site Scripting in Mozilla Firefox

SUMMARY

<<http://www.mozilla.org/>> Firefox is "a fast, full-featured browser that makes browsing more efficient than ever before .

Firefox contains a security vulnerability in the way how it handles cross-domain image dragging, allowing a remote attacker to cause it to execute arbitrary JavaScript.

DETAILS

Vulnerable Systems:

- * Mozilla Firefox version 1.0.1
- * Mozilla Firefox version 1.0

Dragging an image into the address bar will cause Firefox to navigate to the image URL even if it is a JavaScript URL and the page to be navigated from is in a different domain than the page on which the image is shown. This may potentially allow attackers to preform a cross site scripting attack.

Proof of Concept:

```

```

Securiteam: [NEWS] Cross Site Scripting in Mozilla Firefox

A working example of the problem can be located at

<<http://greyhatsecurity.org/vulntests/firefox.htm>>

<http://greyhatsecurity.org/vulntests/firefox.htm>.

ADDITIONAL INFORMATION

The information has been provided by <mailto:paul@greyhats.cjb.net> Paul.

=====

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.