

[NEWS] Browsers' FTP Client can be Used to Send Mail

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-12/0127.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 12/29/04

To: list@securiteam.com

Date: 29 Dec 2004 15:48:39 +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>

Browsers' FTP Client can be Used to Send Mail

SUMMARY

Both Internet Explorer and Konqueror can be tricked into sending mail through its FTP client without any more user interaction than loading a page.

DETAILS

Vulnerable Systems:

- * Internet Explorer version 6 SP1
- * Konqueror version 3.2

Immune Systems:

- * Mozilla Firefox version 1.0

Both Internet Explorer and Konqueror will accept %0a and %0d in URLs. In FTP URLs, it will accept them in the username part of the URL. Due to the similarity between the FTP and SMTP protocols, this can be used to send mail.

Danger:

