

## MSIE->WsOpenJpuInHistory

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2003-09/0146.html>

---

**From:** Liu Die Yu ([liudieyuinchina\\_at\\_yahoo.com.cn](mailto:liudieyuinchina_at_yahoo.com.cn))

**Date:** 09/10/03

Date: 10 Sep 2003 05:59:04 -0000

To: [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)

('binary' encoding is not supported, stored as-is)

WsOpenJpuInHistory

[tested]

Browser Ver

{

MS Internet Explorer: 6.0.2600.0000.xpclnt\_qfe.021108-2107;

Encryption: 128-bit;

Patch:: Q810847;

}

(So, it's far from fully patched.)

OS Ver: "Windows XP Cn ver"

[demo]

refer to:

RefBack-MyPage& BackMyParent-MyPage at [UMBRELLA.MX.TC](http://UMBRELLA.MX.TC)

[exp]

refer to BackMyParent at [UMBRELLA.MX.TC](http://UMBRELLA.MX.TC).

so, the challenge is: "javascript-protocol Url is left  
in the history list"

in this attack:

```
window.open("javascript:[JpuScript]","_search");
```

```
window.open("[VictimUrl]","_search");
```

[greetings]

the Pull, dror, guninski, sandblad and "Friedrich L.Bauer".

of course, mom and dad.

best wishes

-----

from <http://Umbrella.MX.TC> on <http://SafeCenter.NET>