

# 10 Month Old Vulnerability Continues to Be Core For Exploits

*Source:* <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2004-06/0158.html>

---

*From:* Drew Copley ([dcopley\\_at\\_eEye.com](mailto:dcopley_at_eEye.com))

*Date:* 06/10/04

Date: Thu, 10 Jun 2004 10:51:40 -0700

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

<http://lists.netsys.com/pipermail/full-disclosure/2004-June/022498.html>

http-equiv points this out well there.

"All the while conveniently omitting the fact that the so-called 'vulnerability' that does the actual 'sneaking' is a time tested in both demonstration and in the wild 'feature' of Microsoft. The adodb.stream object. Repeatedly proven to be the core and still not addressed for 10 months now.

Microsoft needs to decide whether THAT is in fact a vulnerability or a feature because without it [and a few others] you have nothing. An unremarkable "cross zones," capability as the author of the little news snippet so aptly puts it and who failed to query the manufacturer of this remarkable feature."

...

To protect yourself, you can kill bit this object. It is almost never used.

Windows Registry Editor Version 5.00

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX Compatibility\{00000566-0000-0010-8000-00AA006D2EA4}] "Compatibility Flags"=dword:00000400
```

For those not up on these cross zone scenarios... right now it is possible to run malicious code of one's choosing through html merely if one can find a security hole that breaches from the internet or restricted zone to the local zone.

Another fix, and a really good idea... is to make "My Computer" Zone, aka, "the Local Zone" become visible in your internet properties and harden it done like the Restricted Zone. These two fixes will prevent most unknown IE vulnerabilities -- bottomline.

## SecurityFocus Bugtraq: 10 Month Old Vulnerability Continues to Be Core For Exploits

```
[HKEY CURRENT USER\Software\Microsoft\Windows\CurrentVersion\Internet  
Settings\Zones\0]  
"Flags"= dword:00000001
```

It would be nice if Microsoft included this zone in their settings, say, in XP SP2, and in future w2k3 update. Hiding this kind of thing is a bit like hiding one's safe for one's guns, without the guns in it.

The bar is and does remain low from running code of your choice in Internet Explorer. It has for months. Most of the worms we have seen rely on this. I have no idea why Microsoft has not rushed a fix for this issue. Especially considering the vast numbers of infected people.