

## exploit fix breaks CDO access

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2004-07/0311.html>

---

**From:** Biff ([biffinpitt\\_at\\_comcast.net](mailto:biffinpitt_at_comcast.net))

**Date:** 07/04/04

Date: Sat, 3 Jul 2004 23:05:17 -0700

Hi Folks!

Just an FYI:

I followed a suggested fix that is supposed to eliminate the current "spoofing" exploit and discovered that the fix breaks access to these newsgroups if you use the CDO interface. (web access)

The fix calls for setting "Navigate sub-frames across different domains" to disabled. It seems that these MS ngs use that functionality !!!!!!! Go figure !!!!!!!

With that setting disabled you can open the site but you can't open or read any of the posts. A security fix that won't let you access a security forum. How's that for irony ???

>*From an article at Net-Integration: Credit to AplusWebmaster.*

Microsoft Plugs IE; Report Warns All Browsers At Risk  
– <http://www.techweb.com/wire/story/TWB20040702S0007>  
July 2, 2004 (3:34 p.m. EST) – By Gregg Keizer, TechWeb News

"As if to prove the point that security is like the Dutch boy at the dike, Microsoft on Friday released a stop-gap fix for one of several vulnerabilities that have plagued its Internet Explorer just as a security firm warned that virtually every browser -- not just IE -- can be spoofed by hackers. The update, which Microsoft tagged as "Critical", isn't a patch per se, but rather an change to Windows that disables the ADODB.Stream object within the operating system's Data Access Components (DAC)...Wednesday, Secunia issued a warning saying it had discovered a vulnerability within IE that allowed scammers to spoof, or fake, the content of a site displayed in the browser.

– On Friday, however, the security vendor modified the alert to claim that virtually every browser, from Internet Explorer and Mozilla to Opera and Netscape -- including browsers for both Windows and the Mac OS -- has this flaw. "It's not a code vulnerability," said Secunia's Kristensen, "but a design flaw." The problem stems from how browsers handle frames. "Some time ago, browser designers decided that one site needed to be able to manipulate the content of another, and the functionality was adopted by everyone," said Kristensen. But hackers can use this to inject phony content -- say their own credit card-stealing form -- into a frame of an actual trusted Web site, such as a user's online bank. "In these times of phishing attacks and other scams, this is a problem," said Kristensen. "You're visiting a bank or an e-commerce site, and you're certain of that site, but meanwhile, it's [actually] open in the background to content change by hackers." Internet Explorer users can stymie such spoofing attacks by disabling the "Navigate sub-frames across different domains" setting under Tools/Internet Options/Security.

Secunia offered up a quick test that users can run to see if their current browser is vulnerable to this problem."

>>>

[http://secunia.com/multiple\\_browsers\\_frame...erability\\_test/](http://secunia.com/multiple_browsers_frame...erability_test/)

Biff