

# Re: [Full-Disclosure] New MyDoom exploiting IFRAME

**Source:** <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2004-11/0348.html>

---

**From:** Michal Zalewski ([lcamtuf\\_at\\_ghettot.org](mailto:lcamtuf_at_ghettot.org))

**Date:** 11/10/04

To: n3td3v <[xploitable@gmail.com](mailto:xploitable@gmail.com)>

Date: Wed, 10 Nov 2004 01:39:53 +0100 (CET)

On Tue, 9 Nov 2004, n3td3v wrote:

> *The worst problem with this is microsoft have not announced a patch  
> for the exploit which the virii exploits, so this is wild in every  
> description of the word "wild".*

I never had strong feelings about Microsoft; I took their side on several occasions. Weren't it for my favorable view of their HTML parser, the IFRAME overflow would be likely not discovered by ned two weeks ago.

Now, the way they handled this flaw makes me want turn into a rabid Microsoft basher. That's something.

The problem is known for over two weeks. It was, from the very beginning, obvious how bad it can get. The vendor knew from day zero. An exploit was released. Then a worm. With variants. And yet, the patch is STILL not even planned for Thursday hotfix roundup. There are business customers that are probably starting to feel uneasy about this.

Rather than releasing a patch, Microsoft so far had only initially denied knowing of an exploit (which was a lie, regardless of what its origins were – I myself sent it to SRC and got a confirmation from a live person). They also criticized the discoverer for "irresponsible handling" of the flaw – which couldn't be farther from truth, if you followed the story.

It is reasonable to expect that after CNN and other major news outlet ran a story about the problem, they do feel a considerable pressure from big customers – and yet, they fail to act. This would suggest that their security response capabilities are *\*very\** inadequate at best – they should have the resources to fix an extremely critical problem like this by now, regardless of how much QA is needed on a patch.

I suppose that either all the MSIE coders took a sick leave, or that this is how SRC works. Perhaps Microsoft had taught the world to release responsibly – that is, give them three to six months, sometimes more, to

Full-Disclosure: Re: [Full-Disclosure] New MyDoom exploiting IFRAME

prepare fixes and argue over the impact of an issue – getting to a point where the evidence of their terribly inadequate handling of security problems does not see the daylight, or is even turned into a PR advantage.

Do customers really benefit from a situation where "responsible disclosure" and OIS policies are used to save money by making it easy to under-fund or under-staff security programs, because in most cases it is possible to convince security researchers to gi