

[VulnWatch] Advisory: Internet Explorer Drag and Drop Redeux [CVE-2005-3240] (fwd)

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2006-02/msg00022.html>

- *From:* Matthew Murphy <mattmurphy@xxxxxxxxxx>
 - *Date:* Mon, 13 Feb 2006 18:40:29 -0600
-

-----BEGIN PGP SIGNED MESSAGE-----

Hash: RIPEMD160

My apologies to those who are receiving this late or are otherwise inconvenienced by the staggered release. I had unexpected, last-minute travel issues that interfered somewhat with today's release.

Of note since the initial drafting of the advisory is that Microsoft has released a blog post on the MSRC blog about the vulnerability report, which can be read here:

<http://blogs.technet.com/msrc/archive/2006/02/13/419439.aspx>

The technical/strategic points about the exploit that are raised in the post are indeed accurate (though it references MS05-014, when I believe the correct reference is MS05-008/MS05-013). The exploit has a greater dependence on timing than previous, related attacks. As such, Microsoft's decision not to include this issue in a standalone patch is seemingly justified at this point. However, the point of disagreement with Microsoft remains the choice of release **timeline**.

I released the information about this issue to a trusted colleague (Gadi Evron) for publication today, after what I felt was a reasonable time, in light of my difficulties obtaining internet access.

Though there are disagreements between myself and Microsoft about the nature of this vulnerability, I would like to thank Brian Schafer of the MSRC for adhering to a high level of professionalism and technical accuracy in that post and for continuing to work with me once it was made clear that the issue would imminently become public.

Also of note is that there was a typo in the information I provided originally to SecuriTeam. The proper candidate is CVE-2005-3240, not **3840** as was originally reported by me. SecurityFocus has also informed me that my original BID reservation was a casualty of a data migration and that the proper BID associated with this vulnerability is now BID 16352, which is public in full detail as of this writing.

[VulnWatch] Advisory: Internet Explorer Drag and Drop Redeux [CVE-2005-3240] (fwd)

There have also been some incorrect reports made to SecuriTeam that this issue does not affect Windows XP Service Pack 2. These reports are not correct -- my testing during this investigation was done exclusively on current installations of Windows 2000 and Windows XP. These systems had all service packs applied and all updates installed when tests were performed.

Thanks to Gadi Evron for doing some of my bidding today and taking some of the heat for my fat-fingers.

The final advisory, corrected with the now-accurate references is attached with an armored-format PGP signature inline.

--

"Social Darwinism: Try to make something idiot-proof, nature will provide you with a better idiot."

-- Michael Holstein

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.4.2 (MingW32)

Comment: <http://pgp.mit.edu:11371/pks/lookup?op=get&search=0xB5444D38>

iD8DBQFD8Sb9fp4vUrVETTgRA6VJAKCL+fMJ8b+cIyOPE5Ld+3C2vgCIOgCffRW5
f1H8M88AzB9oMaE32XUUFbk=
=AVSg

-----END PGP SIGNATURE-----

Attachment: [smime.p7s](#)

Description: S/MIME Cryptographic Signature