

Re: [FYI] XP SP2 Security BUG(s) Report

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.inetexplorer.ie6_outlookexpress/2004-08/3

From: cquirke (MVP Win9x) (*cquirkenews_at_nospam.mvps.org*)

Date: 08/22/04

Date: Sun, 22 Aug 2004 11:00:02 +0200

On Sat, 21 Aug 2004 16:58:40 GMT, "Newbie"

>(*BUG 1 of 2*)

>With *XP_SP2*, if you set

>'Internet Options' / 'Security' / 'Scripting' / 'Active Scripting' to 'Prompt',

>both *OE* and *IE* want to prompt you

>for their own internal *ActiveX* scripts,

>not just the scripts in posts or pages.

This is not an SP2 bug, but an indication of poor design in IE and OE.

>Trust me, this gets **really annoying**,

This is true, but do you really want exceptions to monitoring of these risky behaviors purely on the basis that it's "by Microsoft"?

Especially when 3rd-party BHO get to act as the hostile hand within Microsoft's IE and OE glove puppets?

>Pre *SP2*, *OE* & *IE* were able to 'prompt'

>before running each **individual** script

>in emails / news posts / web pages

>with no major problems at all.

Those scripts are (supposed to be running) in the Security Zone that OE, and the URL (default: Internet) are set to. The scripts you are now alerted on are running in local HD "My Computer" zone.

Formally, MS assumed there would be no reason to restrict what the "My Computer" zone can do. Faith was placed in the security zone facility being able to keep material separate. That's why you can't even see the "My Computer" zone as something you can edit in Tools, Options.

SP2 reflects a belated awareness that zones "leak"++ so that it's almost trivial for malware to either hop from Internet or even Restricted to "My Computer", or drop code that can then do whatever it

likes from what is now a "My Computer" zone context.

So SP2 tightens up the hidden "My Computer" zone, even to be paradoxically tighter than more "outermost" zones. And that is what is snaring the way OE and IE operate.

- > *Being able to click on an email / news post / web page*
- > *without letting a script execute has saved my computer*
- > *from malicious scripts on *numerous* occasions...*

Quite. The new changes aim to block what used to get past!

>(*BUG 2 of 2*)

- >*Also, with 'Prompt' turned on for ActiveX and other scripts,*
- >*if you click on a web link in OE, the initial script 'prompt'*
- >*alert often appears *behind* the IE window, and the*
- >*page will not load until you (growl) minimise all*
- >*of the open windows to get to the hidden*
- >*script 'prompt' alert.*

That's a bug, and more serious than it looks. A modal dialog box you can't see can look like a hard lockup, and cause the user to do a bad exit from Windows, which in turn will lose pending registry settings and corrupt data. That XP "fixes" this file system corruption is no comfort, as this just leaves broken files still broken, but no longer detectable as such. Hullo, head-scratching troubleshoot session.

- >*These Script 'Prompt' Alerts*
- >*need to be forced to 'Stay On Top',*
- >*as they were Pre-XP_SP2.*

Aye.

>-----
> Tech Support: The guys who follow the
> 'Parade of New Products' with a shovel.
>-----