

## Re: Microsoft Security Bulletin MS03-040 – 828750

*Source:* <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2003-10/0728.html>

---

*From:* Gary S. Terhune (*grystnews\_at\_mvps.org*)

*Date:* 10/04/03

Date: Sat, 4 Oct 2003 10:28:10 -0700

I think it's an issue of mistaking the cloak for the dagger, Jerry. It's been happening long before now, long before "Swen". It's the nature of malware to be hidden inside something legitimate, or to be cloaked in legitimacy. More recently, the cloak of choice is to appear as much as possible to be an MS Security Patch. Those of us who are familiar with the real McCoy have no difficulty recognizing the fakes. Those who are not should ask those who are before doing *\*anything\** on a computer—and I'm not just talking about what to do with official-sounding emails and posts—the problem of people being screwed by wolves in sheep's clothing is as old as the species, and idiot-proofing is a topic of much wider scope than is appropriate to discuss here—at least not without trimming the X-Post headers.

Back to the topic at hand: Just as the bad guys are depending on knee-jerk reactions to seemingly legitimate and "critical" Security Bulletins to get people to run "patches" that aren't, the persons who complained here are reacting in knee-jerk fashion against anything that bears the characteristics of the more recent malware attacks. I don't think of cross-posting as being inherently bad, just as I don't think of HTML formatting or attachments as inherently bad—I deal with emails and news posts that have all of the above and don't consider them dangerous—just *\*potentially\** so. A quick inspection of headers, file names, and other sane practices (plain text reading, save-to-disk-then-scan-with-AV for attachments, etc.)—such practices have been automatic to me for years, now. Considering all of the "risky" communications I have downloaded, all of the *\*very\** risky sites I have gone to, and all of the less-than-secure systems I've used to do so (because, after all, I am frequently using a "test" machine, or a build in progress, that's lacking in patches, safe configuration, or even AV...) Considering all of that, it's worth noting that I have never had a machine be infected by a virus except when I deliberately chose to do so.

That said, cross-posting has the unfortunate effect of turning several discreet newsgroups into one big, incredibly redundant one. That can be a good thing, that can be a bad thing. I, personally, feel that X-Posting in this case is precisely proper. But it *\*might\** be more acceptable in the current climate to use multiple posting to achieve the same effect. It would at least confine the technology-specific follow-ups to the appropriate groups—not to mention confining the rants to the contexts from which they emanate, <s>.

--

Gary S. Terhune  
MS MVP for Windows 9x  
\*Recommended Help Sites\*  
<http://www.dts-l.org>  
<http://www.mvps.org>  
<http://www.aumha.org>

How to Use the Microsoft Product Support Newsgroups

<http://support.microsoft.com/?pr=newshelp>

+++++

"Jerry Bryant [MSFT]" <jbryant@online.microsoft.com> wrote in message  
news:upMZZBpidHA.616@TK2MSFTNGP11.phx.gbl...

> There is some interesting feedback here to my post. FYI, I personally have  
> been posting our security bulletins and alerts in these newsgroups for over  
> two years now. In fact, I created these security newsgroups (.security and  
> .security.virus) mainly for this purpose. My post is completely consistent  
> with the way I have always posted them. This is the first time anyone had  
> issues with cross posting. I understand the basis of those concerns though  
> and will take them in to consideration. So, in light of recent swen issues  
> in these newsgroups, is it the general feeling of all here that cross  
> posting should not be used to communicate these bulletin releases?

>  
> Microsoft has always maintained that [www.microsoft.com/technet/security](http://www.microsoft.com/technet/security) is  
> authoritative in regards to security issues with our products. This means  
> that even if you are subscribed to our security bulletin notification  
> service, you should verify the validity of that information by going to that  
> site.

>  
> --  
> Regards,

>  
> Jerry Bryant - MCSE, MCDBA  
> Microsoft IT Communities

>  
> Get Secure! [www.microsoft.com/security](http://www.microsoft.com/security)

>  
> This posting is provided "AS IS" with no warranties, and confers no rights.  
> "Jerry Bryant [MSFT]" <jbryant@online.microsoft.com> wrote in message  
> news:015il6hiDHA.3712@tk2msftngp13.phx.gbl...

> > Title: Cumulative Patch for Internet Explorer Execution (828750)  
> > Date: October 3, 2003

> > Software:  
> > Internet Explorer 5.01  
> > Internet Explorer 5.5  
> > Internet Explorer 6.0  
> > Internet Explorer 6.0 for Windows Server 2003  
> > Impact: Run code of attacker's choice.  
> > Maximum Severity Rating: Critical  
> > Bulletin: MS03-040

> > The Microsoft Security Response Center has released Microsoft Security  
> > Bulletin MS03-040

> > What Is It?  
> > The Microsoft Security Response Center has released Microsoft Security  
> > Bulletin MS03-040 which concerns a vulnerability in Internet Explorer.  
> > Customers are advised to review the information in the bulletin, test and  
> > deploy the patch immediately in their environments, if applicable.

> > More information is now available at  
> > <http://www.microsoft.com/technet/security/bulletin/MS03-040.asp>

microsoft.public.security: Re: Microsoft Security Bulletin MS03-040 – 828750

> >  
> > If you have any questions regarding the patch or its implementation after  
> > reading the above listed bulletin you should contact Product Support  
> > Services in the United States at 1-866-PCSafety (1-866-727-2338).  
> > International customers should contact their local subsidiary.  
> >  
> >  
> >  
> > --  
> > Regards,  
> >  
> > Jerry Bryant - MCSE, MCDBA  
> > Microsoft IT Communities  
> >  
> > Get Secure! [www.microsoft.com/security](http://www.microsoft.com/security)  
> >  
> >  
> > This posting is provided "AS IS" with no warranties, and confers no  
> rights.  
> >  
> >  
>  
>