

# Re: M\$ Publisher Update

---

*Source:*

<http://www.tech-archive.net/Archive/Publisher/microsoft.public.publisher.webdesign/2008-02/msg00296.html>

---

- *From:* [analog@xxxxxxxxxxx](mailto:analog@xxxxxxxxxxx)
  - *Date:* Sat, 23 Feb 2008 16:02:08 -0500
- 

I largely agree with your philosophy. I use Norton Ghost to accomplish the same thing. Every machine has at least two hard drives with one reserved for a carbon copy of the C: drive. That has come in handy a couple of times, but I had forgotten to do that when I installed that older patch. Senility is hell...

On Sat, 23 Feb 2008 06:50:49 -0800, "DavidF" <Nope@xxxxxxxxxxx> wrote:

Syd,

I understand what you are saying, and you can color me even more paranoid if you want. I accept the fact that in spite of their best efforts some of the patches that MSFT provides fix one thing, and break another. Rather than take the risk of a patch breaking something on my machines, I have turned off automatic updating. I run a good antivirus and a good firewall (not MSFT), and practice "safe computing", and as a general rule only install SPs, not the individual patches...and even then only when I have to. I figure that by the time a SP is released, a lot of these fix/break patches that are introduced between SPs have been tweaked and fixed. I am sure that isn't always true, but I figure it is less risky to my machines than the hot fixes and patches. I also set a restore point and/or make an image of my C drive before installing SPs. Acronis True Image is a great program...

I refuse to "upgrade" to Vista, to IE7, etc., and I am willing to take my chances by not installing patches, even if MSFT deems them critical. But, I am not willing to suggest other people do the same. It is up to you to evaluate the risk/reward. Don and Mary's comments are probably more relevant to this discussion than mine, as they have installed the patches. Good luck.

DavidF

<[analog@xxxxxxxxxxx](mailto:analog@xxxxxxxxxxx)> wrote in message  
[news:r2pur31fai0b6o2ji7uhncvmhpmi9ad9op@xxxxxxxxxxx](mailto:news:r2pur31fai0b6o2ji7uhncvmhpmi9ad9op@xxxxxxxxxxx)

Yeah, I am aware of those realities. I do not think I have EVER opened a Publisher file on these computers I did not create. Nevertheless, like you say, M\$ calls this a critical update for Office (my profile actually causes a

Re: M\$ Publisher Update

group  
of three related updates to show). Since I got badly burned when I  
installed  
the predecessor to these updates, I cannot help feeling a bit paranoid. I  
do  
like to keep my machines fully updated, but I have a hard time trusting M\$  
after  
that last fiasco that took many hours to fix.

On Fri, 22 Feb 2008 13:27:17 -0800, "DavidF" <Nope@xxxxxxxxxxx>  
wrote:

Syd,

Reference:

<http://www.microsoft.com/technet/security/bulletin/ms08-012.msp>

from that article:

"How could an attacker exploit the vulnerability?

This vulnerability requires that a user open a specially  
crafted Publisher

file with an affected edition of Microsoft Office Publisher.

In an e-mail attack scenario, an attacker could exploit the  
vulnerability

by

sending a specially-crafted file to the user and by convincing  
the user to  
open the file."

Seems to me that unless you open an "infected" Pub file, that  
you do not

need the patch. Consider the workaround proposed:

"Microsoft has tested the following workarounds and states  
in the  
discussion

whether a workaround reduces functionality: Do not open or  
save Microsoft

Office files that you receive from untrusted sources or that  
you receive

unexpectedly from trusted sources. This vulnerability could  
be exploited

when a user opens a specially crafted file."

Du'oh! When was the last time you opened a Pub file that  
you didn't

create? When will be the next?

I am certainly not trying to suggest not installing a patch that  
MSFT

Re: M\$ Publisher Update

considers "critical"...

DavidF

<analog@xxxxxxxxxxxx> wrote in message  
[news:9h3ur3tet1dgc71jco96l8848s7knuitno@xxxxxxxxxxxx](mailto:news:9h3ur3tet1dgc71jco96l8848s7knuitno@xxxxxxxxxxxx)

A couple of years back, Microsoft issued a security update for Publisher, KB894540. Said brilliant bit of code updating had a slight side effect: it rendered almost every .pub file on our half-dozen machines unreadable. The fix was to doctor the registry or roll back to the unpatched state, a daunting task on a dial-up connection due to the necessity to install Office 2000 from scratch and download all the sequential updates.

What was happening was that the security patch saw any older .pub file as potentially malicious code, and there was no easy way to prevent that. The entire experience was a royal PITA!

On February 12, M\$ issued a new set of updates for Office that apparently are aimed at the same malicious code (and some other newer threats as well). On February 13, the KB article was updated to say there are no known issues with these patches. Having gone through hell once before, I was hesitant to install these updates without knowing for certain they would not flag old work product files as malicious, and render them as

Re: M\$ Publisher Update

unreadable.

I contacted M\$, and of course could not get a straight answer. Heck, I could not even get them to understand the question... I then demanded escalation, and here is an email I received:

"Hi Syd ,

"This is Yogesh with Microsoft Technical Support. I am contacting you regarding your case 1058846320.

"I wanted to inform you about the kb articles that you have provided for the updates of Publisher 2000 that these updates are as security updates of the application reading the earlier files as malicious.

"I escalated the issue and found some solution that you can try by:

"Re-save the file publisher files again and the install (kb 946255) the updates which makes the files as new and the updates can be done and the files will not be treated as malicious.

"Please let me know if the steps we discussed have resolved your issue by replying to this e-mail, so that I can update your case accordingly. We would be happy to continue to assist you if necessary."

Is this correct? Has anybody had a problem with these latest updates?

TIA.

Syd

Re: M\$ Publisher Update