

# Suggestions to Microsoft regarding GDI+ patch foolishness

*Source:* <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2004-09/0098.html>

---

*From:* Russ (*Russ.Cooper\_at\_RC.ON.CA*)

*Date:* 09/29/04

Date: Wed, 29 Sep 2004 12:18:22 -0400

To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

Here are some suggestions to Microsoft which may have helped people, and should seriously be considered for the future. They are based on the bold approach they showed with Windows XP SP2. If they do some of these, it will, to me, show that they have actually adopted a committed stance against security problems and prove that a mind-shift is truly upon us as a result of Bill Gates call-to-arms (and the much older work done by so many others, like Jason Garms, Paul Leach, and Steve Lipner.)

Suggestions:

1. The GDI+ Detection Tool was totally useless. It caused more problems than it resolved. Some people thought that deploying it meant they were patched. Others were at a loss as to what it was telling them to do. Further, it established a rather disturbing precedence. At no time in the past has Windows Update offered up something which didn't actually fix the problem.

Don't do something like this again.

2. Regardless the variety of technologies involved in getting systems patched, I cannot believe that it would be impossible to write a single installation package. So what if it has to call to multiple patch installer programs. This should have been done.

3. Forcing an entire service pack on people who are only 1 service pack out of date is against messaging I've previously heard from Microsoft (I believe.) Why people who have, for example, Office 2003 RTM upgrade to SP1 is contrary to support policies (again, I believe.) The same can be said of .Net Framework installations.

It should not now become the policy of Microsoft to force people to install an entire service pack in order to get secured? Even if you don't force people, it should not be your first recommendation (as in the case of Office Update?)

This is a *\*Critical\** vulnerability, patching quickly, easily, and verifiably is crucial.

4. You should be hosting a site providing information on 3rd party vendors status wrt GDIPlus.dll. They're using your DLL, and as I've previously complained about, this is something you should track. Not every single piece of freeware, but the commercially marketed products would be a good start.

You should have provided a means by which every vulnerable version of your component could be discovered, and here's the bold part, give users an option to "disable" all of them you cannot fix. Yes, this

## NT-Bugtraq: Suggestions to Microsoft regarding GDI+ patch foolishness

would break those applications, but it would've been the users choice (IOWs, they'd have to "opt-in" to do this.) At the very least, Administrators would have been able to sit back and say... "We're not going to get hit, but we will have to deal with the support calls."

5. You should get your act together regarding the DLL Help Database. This complaint is now more than 5 years old!

<<http://support.microsoft.com/default.aspx?scid=/servicedesks/fileversion/dllinfo.asp&SD=MSDN>>

<<http://tinyurl.com/1mgk>>

<http://support.microsoft.com/default.aspx?scid=http%3a%2f%2fsupport.microsoft.com%2fservicedesks%2ffileversion>

The only products you list including GDIPLUS.DLL in according to it;

SBS 2003  
Visio 2002  
Visual Foxpro 8.0  
VS.Net 2002  
VS.Net 2003  
Windows Server 2003  
Windows XP

This is ridiculous. Worse, that dB contains incorrect relative paths and makes no mention of which version is vulnerable or isn't.

So much could be done with this database to assist Administrators in figuring out what's what on their systems, yet its been left in a completely unreliable state for years. Given that you make a product that keeps track of software versioning, one has to wonder why the DLL Help Database couldn't be made reliable.

Let's all hope they step up to the bar.

Cheers,  
Russ – Senior Scientist/NTBugtraq Editor  
TruSecure Corporation

--

NTBugtraq Editor's Note:

Want to reply to the person who sent this message? This list is configured such that just hitting

--