Subject: Everyone Read - Windows WMF Vulnerability Patch
Posted by light on Mon, 02 Jan 2006 21:25:20 GMT
View Forum Message <> Reply to Message

Last week a vulnerability was found in all versions of windows that allows people to execute arbitrary code using a buffer over-run in Windows Metafiles.

WMF files are images, so can be placed on any website or email and can be used to attack your system.

Please, everyone read: http://grc.com/sn/notes-020.htm
Use this to see if your system is vulnerable:
http://www.hexblog.com/2006/01/wmf_vulnerability_checker.htm l
Use this to 3rd party patch to secure it:
http://www.hexblog.com/security/files/wmffix_hexblog13.exe

More technical details can be found here: http://www.f-secure.com/weblog/

EDIT:

Due to over-use, the hexblog website has been suspeneded. New Download links hosted on GRC.com

The Checker: http://www.grc.com/miscfiles/wmf_checker_hexblog.exe
and The Patcher: http://www.grc.com/miscfiles/wmffix_hexblog14.exe

EDIT 2:

A revised list of vulnerable OS's. Bascially the two main ones are XP and Server 2003.
http://blog.ziffdavis.com/seltzer/archive/2006/01/03/39684.a spx

F-Secure RSS Feed:

Larry Seltzer from eWeek has been doing lots of additional testing against older versions of Windows and bad WMF files.He has just blogged his interesting findings:...in a practical sense, only Windows XP and Windows Server 2003 (in all their service pack levels) are vulnerable to the WMF flaw.
...all versions of Windows back to 3.0 have the vulnerability in GDI32.

Except for Windows XP and Windows Server 2003, no Windows versions, in their default configuration, have a default association for WMF files, and none of their Paint programs or any other standard programs installed with them can read WMF files...So the vulnerability is there on all platforms but it seems that only Windows XP and 2003 are easily exploitable. Unfortunately this still means that majority of Windows computers out there are vulnerable right now. And at least Windows 2000 becomes vulnerable if you're using many of the available third party image handling programs to open image files. On 03/01/06 At 07:29 AMhttp://www.f-secure.com/weblog/#00000764