

# InfoTech: Microsoft announce IE in W2220 and XP may allow hackers access to files on PC

If you are one of those rebels who sticks doggedly to Windows 2000 or XP for the simple reason that your business operations do not require the later versions of the operating system - or applications software - Microsoft has news for you. Even if you've got the latest versions of 2000 or XP, you've got a problem. Of course, if you had upgraded to Vista or Windows 7 when Microsoft told you, you'd be safe. But it's the wording of the that should panic company directors: Microsoft has exposed you to massive legal liability.

A warning from Microsoft yesterday (they call them "Security Advisory" says that a "vulnerability in Internet Explorer could allow information disclosure."

This wording is both obscure and calculated to terrify.

First, what it really means is this: in some circumstances which Microsoft has been able to replicate, hackers are able to break into a PC via the browser and steal files.

That's bad enough, but the terrifying bit is "information disclosure."

This is the kind of language that is used by people who draft legislation. And in this context it means this: by Microsoft issuing its "advisory" all companies that operate 2000 or XP (or server 2003) software are now on notice that data is not secure. And so by failing to do something about it, they are failing to take proper care of data.

And if data is lost because the company fails to take proper care of it, then under data protection laws in many countries and even individual US states such as California, there are very - VERY - substantial penalties if it turns out that data is lost. The UK, for example, has recently announced that negligent loss of data will incur a civil penalty (i.e. imposed without trial) of up to GBP500,000 per instance.

The following is extracted from the Microsoft announcement:

*"Our investigation so far has shown that if a user is using a version of Internet Explorer that is not running in Protected Mode an attacker may be able to access files with an already known filename and location. These versions include Internet Explorer 5.01 Service Pack 4 on Microsoft Windows 2000 Service 4; Internet Explorer 6 Service Pack 1 on Microsoft Windows 2000 Service Pack 4; and Internet Explorer 6, Internet Explorer 7, and Internet Explorer 8 on supported editions of Windows XP Service Pack 2, Windows XP Service Pack 3, and Windows Server 2003 Service Pack 2. Protected Mode prevents exploitation of this vulnerability and is running by default for versions of Internet Explorer on Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008.*

*"The vulnerability exists due to content being forced to render incorrectly from local files in such a way that information can be exposed to malicious websites... An attacker who successfully exploited this vulnerability could gain the same user rights as the local user. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative user rights."*

The company says that the problem can be limited, but does not say it can be prevented, by running "protected mode" for IE under Vista. It recommends firewalls, anti-virus scans and other measures and also running websites and html versions of Microsoft email programs in Restricted Mode - which severely limits their operations.

[Microsoft warning notice](#)