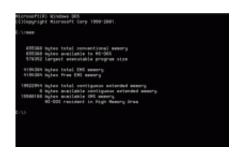# Microsoft to patch 17-year-old bug

February 8 2010, by Lin Edwards

(PhysOrg.com) -- Microsoft's February security update will include a patch for a bug that dates back to Windows NT 3.1, which was released in July 1993. The vulnerability has been present but undetected in every 32-bit version of Windows since 1993, including Windows XP, Vista, Windows 2000, Server 2003 and 2008, and the newest version: Windows 7.

A security researcher for Google, Tavis Ormandy, found several flaws in the Virtual DOS Machine (VDM) utility that enables more recent releases of Windows to run old DOS and 16-bit software. The bug has the potential to enable an unprivileged 16-bit program to gain system privileged access level to the PC, which would allow attackers to get their own code to run. Ormandy found the bug and reported it to Microsoft over seven months ago and published a workaround, but a patch has not been ready until now.

The 17-year-old bug affects only Windows 32-bit versions and does not affect 64-bit machines, which does not have support for 16-bit applications. Microsoft has released a security advisory, which says the company is not aware of any attacks involving the vulnerability, and most users are at low risk, apparently because local access to the computer is required.

Among the 25 other patches included in this month's security update are five "critical" vulnerabilities that could allow an attacker to hijack a PC running Windows and force it to run their own programs. The update also fixes bugs in Microsoft Office 2003 and XP, and Office 2004 for Apple Macintosh.

© 2010 PhysOrg.com