

Microsoft Corp. today released an unprecedented number of software security updates to plug flaws in its products, including seven "critical" defects that it said hackers could use to hijack vulnerable computers running the Windows operating system.

The free updates, available at Microsoft's [Windows Update Web site](#), are designed to fix at least 21 new vulnerabilities, several of which reside on nearly every version of the Windows operating system and affect hundreds of millions of computers.

Microsoft rated seven of the flaws critical, its most dire warning, saying that the holes could allow attackers to take control of affected PCs just by convincing users to visit certain Web sites. Three of the flaws reside on the company's Internet Explorer Web browser.

"I've never seen Microsoft release this many patches at one time," said Darwin Herdman, chief technology officer at Red Siren, a Pittsburgh based Internet security company. "The install base for these flaws is enormous."

Oliver Friedrichs, senior manager of security response at Cupertino, Calif.-based Internet security company Symantec Corp., said he is worried about a group of four flaws in the way Windows processes images and other digital content. These vulnerabilities, which apply to nearly all versions of Windows, pose the greatest danger for Windows home users, Friedrichs said.

Other computer experts worried about the security holes affecting software products mainly used in large and mid-sized business. Russ Cooper, chief scientist at Herndon, Va.-based TruSecure Corp., pointed to the patch intended to plug a critical software flaw in Microsoft's Server 2003 operating system and Exchange Server 2003, a program that manages incoming and outgoing e-mail.

The flaw in Exchange could allow hackers to take control over unsuspecting computer users' mail servers, forcing the computers to send spam and "phishing" e-mail scams.

"There are all kinds of bad things you could do with this flaw since Exchange servers are installed in some pretty high-profile companies," Cooper said.

Nearly all of the patches released today that affect Windows XP ([news - web sites](#)) -- the operating system of choice of more than 200 million home computer users -- were included in Service Pack 2, a massive security update Microsoft released in August. Consequently, XP users who have installed Service Pack 2 only must install two of the patches made available Tuesday.

One of those patches covers an Internet Explorer security hole rated "important" by Microsoft. The other is a re-release of a fix Microsoft released last month to mend a problem in the way the Windows operating system and Microsoft Office products process digital image files that could let attackers take control of affected PCs. Hackers have been exploiting the problem to conduct

relatively minor attacks for weeks now. Microsoft said it re-issued the patch because it did not install properly on many PCs.

That re-issue also was designed to make it easier for people to install last month's fix. The September patch was included in Service Pack 2, and was made available through Microsoft's Windows Update site and its automatic update service. But many security experts criticized Microsoft for not making it clear that people with Office XP installed still needed to visit Microsoft's Office Update Web site to install an additional fix to be completely protected.

As a result of that feedback, Microsoft has agreed to make this particular patch for its Office XP patch available via its Windows Update site, said Stephen Toulouse, Microsoft's security program manager. Toulouse said Microsoft plans to roll out a one-stop Microsoft Update site sometime next year that provides automatic updates for all of the company's products from a single source.