CMP United Business Media
Network Computing
Driving IT Decisions

Windows Vulnerabilities: Coming to a Cisco Device Near You

February 4, 2002
By Greg Shipley

Let's face it, Microsoft is an easy target when it comes to security problems -- vulnerability after vulnerability, worm after worm, hole after hole. Companies are losing millions of dollars as they scurry to prevent the next piece of "malware" from reducing their data to a pile of contaminated rubble. Not only are Microsoft Internet Explorer, Outlook, Internet Information Server and Windows XP falling victim to an endless onslaught of disastrous security holes, but the trend doesn't seem to be improving.

Take, for example, the latest Windows XP Universal Plug and Play fiasco. Back in October, Jim Allchin, a Microsoft group VP, said in an interview, "We have gone through all [XP] code and, in an automated way, found places where there could be buffer overflow, and those have been removed in "Windows XP." Yet just two months later, a nasty buffer overflow in XP's UPnP service affected virtually every installation of Windows XP on the planet. So much for that automated search, Jim.

Windows Inside?

Here's something I don't hear people discussing very often: Where Windows products go, vulnerabilities will follow. While wicked OS holes are making mainstream headlines, who's keeping watch where all the other "Windows-based solutions" lurk? What about turnkey solutions? Or embedded systems? Or, much to my chagrin, Cisco switches and VoIP products?

That's right. Under the hood of some of those hip new "blades" for your Cisco switches and VoIP units lies a PC -- a PC that is running Microsoft Windows. If this makes you nervous, get in line. If it doesn't, start worrying now. Think about it: When was the last time a virus took out your phone system? Migrate to a VoIP solution dependent on Windows and you may come to learn a whole new meaning for the word convergence. After the next Nimda or Code Red rips through your e-mail and Web servers, your new VoIP phone system could fall victim as well. Although I understand the many advantages in Microsoft-based development environments, as a consumer, if I wanted a VoIP solution dependent on Microsoft technology, I'd ask Microsoft for it. But I don't.

To be fair, Cisco isn't the only company plagued by Microsoft-based security problems. We're seeing more appliances and turnkey solutions shipping with strong dependencies on the Microsoft Web platform. Making matters worse, these bundled solutions introduce yet another problem to burdened IT staffs: the problem of third-party patching. Although you can download a patch for the latest IIS hole and apply it to your Web servers, the rules change when you don't have the same kind of administrative access to that turnkey appliance or that Catalyst switch blade. Unfortunately, your hands are tied, and your turnkey systems just became sitting ducks.

Vendors must realize that security issues don't relate to security products alone. If you're going to introduce a system into my network, that system had better be secure. If it's not, you're introducing a liability into my organization. Vendors also need to wake up when it comes to partnering. Putting IIS -- the Web server with the worst security record in the history of the Internet -- on an embedded platform is just plain stupid.

Finally, there's little chance of vendors changing their ways unless consumers start requesting specific changes. So before you sign that next PO, do your IT and security staffs a favor: Take a moment to look under the hood and ask yourself if the purchase is adding an asset or a liability to your organization. Remember your phone systems can be hit by worms and your Cisco hardware has Microsoft products running on it. Me? I'm waiting for hell to freeze over any day now.

Send your comments on this column to Greg Shipley at gshipley@neohapsis.com.