ASA-15-0608-4: Remote Code Execution Vulnerability in Server Service Software

Vulnerability summary

Severity rating:	Critical
Date Published:	August 8, 2006
Software Vendor:	Microsoft
Affected Software:	Microsoft Server Service
Affected OS:	Windows XP (all), Windows Server 2003 (all), Microsoft Windows XP Professional x64 Edition, Windows 2000 (all), Windows 98 (incl. SE), Windows Millennium Edition (ME)
Unaffected with:	-
Vulnerability class:	Remote Code Execution
Status:	Fixed

Vulnerability details

Technical brief:
A remote code execution vulnerability exists in Microsoft Server Service software that can lead to the execution of arbitrary code on a vulnerable machine.

A critical vulnerability in Server Service software and similar types of errors in Windows operating system code can be preemptively mitigated through the use of personal firewall software to control your computer's network connections and screen the data sent and received by the computer.

Too often, software vulnerabilities are found and removed only after someone has actively exploited them; hackers have a window of opportunity between vulnerability discovery and vendor patch availability to wreak chaos on unpatched systems. Even if the vulnerability has been promptly reported to the vendor and a patch issued quickly, there is no sure way to determine whether this vulnerability has been known and taken advantage of in the past by cybercriminals focused on identifying and exploiting flawed software.

The latest Microsoft advisory, Security Bulletin MS06-040, warns of a flawed Windows component called Server Service. Exploiting this flaw would enable a attacker to take complete control over the system, including stealing documents, launching unauthorized programs, and sending out spam. Although Microsoft has issued a timely fix, if your system has not been updated, you will run a high risk of infection every time you connect to the Internet.
Hot on the heels of the vulnerability being announced came the first exploits (malware that exploits the underlying vulnerability) - a fast-propagating worm named Win32/Graweg.

While all Windows users should update their systems as soon as possible using the Windows Update service, Outpost users can be confident that they are automatically protected against

these exploits. Outpost Firewall Pro automatically closes the exposed connection ports over which the vulnerable service might be accessed.

Vendor reference information:
Details pertaining to the problem are available here:
http://www.microsoft.com/technet/security/bulletin/MS06-040.mspx

General mitigation recommendations:
Install the latest vendor patches, available at http://windowsupdate.microsoft.com.
Block TCP ports 139 and 445 at the firewall to prevent access from external networks (IP addresses falling outside of your trusted range).

How Outpost Firewall Pro protects you:
Outpost Firewall Pro automatically prevents connections through the affected ports from the Internet. Additionally, Outpost protects your system from unauthorized access and intrusions, and alerts you if malicious code attempts to execute or access the network.

Disclaimer:
The information contained in this advisory is believed to be accurate at the time of publishing based on currently-available information. Use of this information signifies acceptance for use in an AS IS condition. There are no warranties with regard to this information. Agnitum Ltd does not accept any liability for any direct, indirect, or consequential loss or damage arising from use of, or reliance on, this information.

Source:
http://www.agnitum.com/news/security_advisories/advisory15.php