

## Microsoft Windows Server 2003 Service Pack 2

Microsoft released Service Pack 2 on the 13th March. The majority of the patches are relatively old, however this service pack should be applied as part of your normal patch cycle.

The security bulletins addressed by SP2 include:

- MS04-034: Vulnerability in compressed (zipped) folders could allow code execution
- MS05-025: Cumulative security update for Internet Explorer
- MS05-032: Vulnerability in Microsoft agent could allow spoofing
- MS05-020: Cumulative security update for Internet Explorer
- MS05-040: Vulnerability in Telephony service could allow remote code execution
- MS05-026: A vulnerability in HTML Help could allow remote code execution
- MS05-027: Vulnerability in Server Message Block could allow remote code execution
- MS05-033: Vulnerability in Telnet client could allow information disclosure
- MS05-052: Cumulative security update for Internet Explorer
- MS05-038: Cumulative security update for Internet Explorer
- MS05-042: Vulnerabilities in Kerberos could allow denial of service, information disclosure, and spoofing
- MS05-039: Vulnerability in Plug and Play could allow remote code execution and elevation of privilege
- MS05-041: Vulnerability in Remote Desktop Protocol could allow denial of service
- MS05-049: Vulnerabilities in the Windows shell could allow for remote code execution
- MS05-036: Vulnerability in Microsoft Color Management Module could allow remote code execution
- MS05-051: Vulnerabilities in MS DTC and COM+ could allow remote code execution
- MS05-050: Vulnerability in DirectShow could allow remote code execution
- MS05-045: Vulnerability in Network Connection Manager could allow denial of service
- MS05-054: Cumulative security update for Internet Explorer

- MS06-002: Vulnerability in embedded Web fonts could allow remote code execution
- MS06-015: Vulnerability in Windows Explorer could lead to remote code execution
- MS06-004: Cumulative security update for Internet Explorer
- MS06-025: Vulnerability in Routing and Remote Access could allow remote code execution
- MS06-008: Vulnerability in WebClient could allow remote code execution
- MS06-013: Cumulative security update for Internet Explorer
- MS06-001: Vulnerability in graphics rendering engine could allow remote code execution
- MS06-007: Vulnerability in TCP/IP could allow denial of service
- MS06-036: A vulnerability in the DHCP Client Service could allow remote code execution
- MS06-030: Vulnerability in Server Message Block could allow elevation of privilege
- MS06-021: Cumulative security update for Internet Explorer
- MS06-035: Vulnerability in Server service could allow remote code execution
- MS06-023: Vulnerability in Microsoft JScript could allow remote code execution
- MS06-051: Vulnerability in the Windows kernel could result in remote code execution
- MS06-034: Vulnerability in Internet Information Services that use Active Server Pages could allow remote code execution
- MS06-024: Vulnerability in Windows Media Player could allow remote code execution
- MS06-032: Vulnerability in TCP/IP could allow remote code execution
- MS06-022: Vulnerability in ART image rendering could allow remote code execution
- MS06-042: Cumulative security update for Internet Explorer
- MS06-068: Vulnerability in Microsoft Agent could allow remote code execution
- MS06-043: Vulnerability in Microsoft Windows could allow remote code execution
- MS06-050: Vulnerabilities in Microsoft Windows Hyperlink Object Library could allow remote code execution

- MS06-041: Vulnerability in DNS resolution could allow remote code execution
- MS06-053: Vulnerability in Indexing Service could allow cross-site scripting
- MS06-045: Vulnerability in Windows Explorer could allow remote code execution
- MS06-040: Vulnerability in Server service could allow remote code execution
- MS06-046: Vulnerability in HTML Help could allow remote code execution
- MS06-067: Cumulative security update for Internet Explorer
- MS06-064: Vulnerabilities in TCP/IP IPv6 could allow denial of service
- MS06-057: Vulnerability in Windows Explorer could allow remote code execution
- MS06-063: Vulnerability in Server Service could allow denial of service
- MS06-078: Vulnerability in Windows Media Format could allow remote code execution
- MS06-076: Cumulative security update for Outlook Express
- MS06-066: Vulnerability in the Client Service could allow remote code execution
- MS06-061: Vulnerabilities in Microsoft XML Core Services could allow remote code execution
- MS06-065: Vulnerability in Windows Object Packager could allow remote execution
- MS06-072: Cumulative security update for Internet Explorer
- MS06-055: Vulnerability in Vector Markup Language could allow remote code execution
- MS06-077: Vulnerability in Remote Installation Services could allow remote code execution
- MS06-074: Vulnerability in Simple Network Management Protocol (SNMP) could allow remote code execution
- MS06-075: Vulnerability in Windows could allow elevation of privilege
- MS07-004: Vulnerability in Vector Markup Language could allow remote code execution

Further details can be found at :

<http://www.microsoft.com/technet/windowsserver/default.msp>