
RAPID7
UNIFIED VULNERABILITY MANAGEMENT


Simplicity Defined
FORTRESS

Report Card

1. Node Vulnerability Report Card

1.1. 10.2.51.250 (iml-accounting)

1.1.1. Critical Vulnerabilities

Name	Status	Confirmed By
Missing Oracle Critical Patch Update (CPU) for October 2009	Vulnerable Version	Running vulnerable Oracle service: Oracle 10.1.0.3.0.0.
Missing Oracle Critical Patch Update (CPU) for April 2005	Vulnerable Version	Running vulnerable Oracle service. Based on the result of the "Oracle DBMS_METADATA SQL Injection" test, this node is vulnerable to this additional issue as well.
Missing Oracle Critical Patch Update (CPU) for April 2006	Vulnerable Version	Running vulnerable Oracle service. Based on the result of the "Oracle MDSYS SDO_PRIDX SQL Injection" test, this node is vulnerable to this additional issue as well.
Missing Oracle Critical Patch Update (CPU) for April 2006	Vulnerable Version	Running vulnerable Oracle service. Based on the result of the "Oracle MDSYS SDO_PRIDX SQL Injection" test, this node is vulnerable to this additional issue as well.
Missing Oracle Critical Patch Update (CPU) for April 2007	Vulnerable Version	Running vulnerable Oracle service. Based on the result of the "Oracle DBMS_CDC_PUBLISH SQL Injection" test, this node is vulnerable to this additional issue as well.
Missing Oracle Critical Patch Update (CPU) for April 2007	Vulnerable Version	Running vulnerable Oracle service. Based on the result of the "Oracle DBMS_CDC_IPUBLISH Buffer Overflow" test, this node is vulnerable to this additional issue as well.
Missing Oracle Critical Patch Update (CPU) for April 2007	Vulnerable Version	Running vulnerable Oracle service. Based on the result of the "Oracle DBMS_AQADM_SYS SQL Injection" test, this node is vulnerable to this additional issue as well.
Missing Oracle Critical Patch Update (CPU) for April 2008	Vulnerable Version	Running vulnerable Oracle service. Based on the result of the "Oracle SDO_IDX CMT_IDX_CHNGS SQL Injection" test, this node is vulnerable to this additional issue as well.
Missing Oracle Critical Patch Update (CPU) for January 2007	Vulnerable Version	Running vulnerable Oracle service. Based on the result of the "Oracle

Name	Status	Confirmed By
		DBMS_CAPTURE_ADM_INTERNAL Buffer Overflow" test, this node is vulnerable to this additional issue as well.
Missing Oracle Critical Patch Update (CPU) for January 2007	Vulnerable Version	Running vulnerable Oracle service. Based on the result of the "Oracle DBMS_REPCAT_UNTRUSTED UNREGISTER_SNAPSHOT Buffer Overflow" test, this node is vulnerable to this additional issue as well.
Missing Oracle Critical Patch Update (CPU) for January 2007	Vulnerable Version	Running vulnerable Oracle service. Based on the result of the "Oracle DBMS_LOGREP_UTIL Buffer Overflow" test, this node is vulnerable to this additional issue as well.
Missing Oracle Critical Patch Update (CPU) for January 2008	Vulnerable Version	Running vulnerable Oracle service. Based on the result of the "Oracle XDB.XDB_PITRIG_PKG PITRIG_DROP and PITRIG_TRUNCATE Procedure Vulnerabilities" test, this node is vulnerable to this additional issue as well.
Missing Oracle Critical Patch Update (CPU) for July 2006	Vulnerable Version	Running vulnerable Oracle service. Based on the result of the "Oracle KUPW$WORKER MAIN SQL Injection" test, this node is vulnerable to this additional issue as well.
Missing Oracle Critical Patch Update (CPU) for July 2006	Vulnerable Version	Running vulnerable Oracle service. Based on the result of the "Oracle KUPM$MCP MAIN SQL Injection" test, this node is vulnerable to this additional issue as well.
Missing Oracle Critical Patch Update (CPU) for October 2005	Vulnerable Version	Running vulnerable Oracle service. Based on the result of the "Oracle SDO_TUNE EXTENT_OF SQL Injection" test, this node is vulnerable to this additional issue as well.
Missing Oracle Critical Patch Update (CPU) for October 2006	Vulnerable Version	Running vulnerable Oracle service. Based on the result of the "Oracle DBMS_XDBZ ENABLE_HIERARCHY SQL Injection" test, this node is vulnerable to this additional issue as well.
Missing Oracle Critical Patch Update (CPU) for October 2007	Vulnerable Version	Running vulnerable Oracle service. Based on the result of the "Oracle LT FINDRICSET SQL Injection" test, this node is vulnerable to this additional issue as well.
OpenSSH X11 Cookie Local Authentication Bypass Vulnerability	Vulnerable Version	Running vulnerable SSH service: OpenSSH 4.3p2.
Oracle Obsolete Version	Vulnerable Version	Running vulnerable Oracle service: Oracle 10.1.0.3.0.0.

Name	Status	Confirmed By
Oracle SDO_IDX CMT_IDX_CHNGS SQL Injection	Exploited	Running vulnerable Oracle service. 1: ORA-29400: data cartridge error 2: ORA-01756: quoted string not properly terminated
Oracle LT FINDRICSET SQL Injection	Exploited	Running vulnerable Oracle service. 1: ORA-01756: quoted string not properly terminated
Oracle XDB.XDB_PITRIG_PKG PITRIG_DROP and PITRIG_TRUNCATE Procedure Vulnerabilities	Exploited	Running vulnerable Oracle service. 1: ORA-00604: error occurred at recursive SQL level 1 2: ORA-00933: SQL command not properly ended

1.1.2. Severe Vulnerabilities

Name	Status	Confirmed By
Missing Oracle Critical Patch Update (CPU) for October 2008	Vulnerable Version	Running vulnerable Oracle service. Based on the result of the "Oracle SYS.LTADM AreThereDiffs SQL Injection" test, this node is vulnerable to this additional issue as well.
Oracle DBMS_AQADM_SYS SQL Injection	Exploited	Running vulnerable Oracle service. 1: ORA-24047: invalid agent name ' || -- , agent name should be of the... 2: ORA-01756: quoted string not properly terminated
Oracle DBMS_CAPTURE_ADM_INTERNAL Buffer Overflow	Exploited	Running vulnerable Oracle service. 1: ORA-01948: identifier's name length (31) exceeds maximum (30)
Oracle DBMS_CDC_IPUBLISH Buffer Overflow	Exploited	Running vulnerable Oracle service. 1: ORA-00600: internal error code, arguments: [changeTableCache-1], [], [...
Oracle DBMS_CDC_PUBLISH SQL Injection	Exploited	Running vulnerable Oracle service. 1: ORA-06550: line 1, column 65: 2: PLS-00103: Encountered the symbol "', lockhandle => :1); end;" wh...
Oracle DBMS_LOGREP_UTIL Buffer Overflow	Exploited	Running vulnerable Oracle service: Oracle 10.1.0.3.0.0. 1: No more data to read from socket

Name	Status	Confirmed By
Oracle DBMS_METADATA SQL Injection	Exploited	Running vulnerable Oracle service. 1: ORA-00904: "FOO": invalid identifier
Oracle DBMS_REPCAT_UNTRUSTED UNREGISTER_SNAPSHOT Buffer Overflow	Exploited	Running vulnerable Oracle service: Oracle 10.1.0.3.0.0. 1: No more data to read from socket
Oracle DBMS_XMLSCHEMA Buffer Overflow	Exploited	Running vulnerable Oracle service. 1: No more data to read from socket
Oracle DBMS_XMLSCHEMA_INT Buffer Overflow	Exploited	Running vulnerable Oracle service. 1: No more data to read from socket
Oracle KUPM$MCP MAIN SQL Injection	Exploited	Running vulnerable Oracle service. 1: ORA-39085: cannot update job ' for user 2: ORA-06512: at "SYS.DBMS_SYS_ERROR", line 95 3: ORA-06512: at "SYS.KUPV$FT_INT", line 2546 4: ORA-01756: quoted string not properly terminated
Oracle KUPW$WORKER MAIN SQL Injection	Exploited	Running vulnerable Oracle service. 11: ORA-06512: at "SYS.KUPW$WORKER", line 1243 12: ORA-39086: cannot retrieve job information 13: ORA-06512: at "SYS.DBMS_SYS_ERROR", line 79 14: ORA-06512: at "SYS.KUPV$FT_INT", line 1684 15: ORA-01756: quoted string not properly terminated
Oracle SDO_TUNE EXTENT_OF SQL Injection	Exploited	Running vulnerable Oracle service. 1: ORA-01756: quoted string not properly terminated
Oracle SYS.LTADM AreThereDiffs SQL Injection	Exploited	Running vulnerable Oracle service. 1: ORA-01756: quoted string not properly terminated
OpenSSH X11 Fowarding Information Disclosure Vulnerability	Vulnerable Version	Running vulnerable SSH service: OpenSSH 4.3p2.

Name	Status	Confirmed By
Oracle MDSYS SDO_PRIDX SQL Injection	Exploited	Running vulnerable Oracle service. 1: ORA-01756: quoted string not properly terminated
Oracle DBMS_XDBZ ENABLE_HIERARCHY SQL Injection	Exploited	Running vulnerable Oracle service. 1: ORA-01756: quoted string not properly terminated
OpenSSH CBC Mode Information Disclosure Vulnerability	Vulnerable Version	Running vulnerable SSH service: OpenSSH 4.3p2.
OpenSSH "X11UseLocalhost" X11 Forwarding Session Hijacking Vulnerability	Vulnerable Version	Running vulnerable SSH service: OpenSSH 4.3p2.

1.1.3. Moderate Vulnerabilities

No moderate vulnerabilities were reported.

1.2. 10.2.53.211 (iml-desktop2)

1.2.1. Critical Vulnerabilities

Name	Status	Confirmed By
Microsoft DirectShow Streaming Video ActiveX Control Buffer Overflow	Exploited	ActiveX control with GUID 011B3619-FE63-4814-8A84-15A194CE9CE3 is installed
Microsoft Office Web Components Code Execution Vulnerability	Exploited	ActiveX control with GUID 0002E559-0000-0000-C000-000000000046 is installed
MS08-007: Vulnerability in WebDAV Mini-Redirector Could Allow Remote Code Execution (946026)	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 Based on the result of the "Windows XP Service Pack 3 (KB936929)" test, this node is vulnerable to this additional issue as well. C:\WINDOWS\system32\drivers\mrxdav.sys has version 5.1.2600.2180 C:\WINDOWS\system32\drivers\mrxdav.sys - file does exist
MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 C:\WINDOWS\system32\netapi32.dll has version 5.1.2600.2180 C:\WINDOWS\system32\netapi32.dll - file does exist

Name	Status	Confirmed By
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WindowsCSDVersion - contains unexpected value 512
MS09-042: Vulnerability in Telnet Could Allow Remote Code Execution	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 C:\WINDOWS\system32\telnet.exe has version 5.1.2600.2180 C:\WINDOWS\system32\telnet.exe - file does exist HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WindowsCSDVersion - contains unexpected value 512
Mozilla Firefox CSS Reference Counter Code Execution Vulnerability	Vulnerable Version	Vulnerable software installed: Mozilla Firefox 2.0.0.2
Mozilla Firefox Multiple Vulnerabilities Fixed in versions 2.0.0.17 and 3.0.2	Vulnerable Version	Vulnerable software installed: Mozilla Firefox 2.0.0.2
Mozilla Firefox Multiple Vulnerabilities Fixed in versions 2.0.0.18 and 3.0.4	Vulnerable Version	Vulnerable software installed: Mozilla Firefox 2.0.0.2
Mozilla Firefox Multiple Vulnerabilities Fixed in versions 2.0.0.19 and 3.0.5	Vulnerable Version	Vulnerable software installed: Mozilla Firefox 2.0.0.2
Wireshark Multiple Vulnerabilities Fixed in version 1.0.7	Vulnerable Version	Vulnerable software installed: The Wireshark developer community, http://www.wireshark.org Wireshark 0.99.6a
Mozilla Firefox Multiple Vulnerabilities Fixed in 3.0.7	Vulnerable Version	Vulnerable software installed: Mozilla Firefox 2.0.0.2
Mozilla Firefox Multiple Vulnerabilities Fixed in 3.0.8	Vulnerable Version	Vulnerable software installed: Mozilla Firefox 2.0.0.2
MS07-061: Vulnerability in Windows URI Handling Could Allow Remote Code Execution (943460)	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 Based on the result of the "Windows XP Service Pack 3 (KB936929)" test, this node is vulnerable to this additional issue as well. C:\WINDOWS\system32\shell32.dll has version 6.0.2900.2180 C:\WINDOWS\system32\shell32.dll - file does exist
MS08-021: Vulnerabilities in GDI Could Allow	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2

Name	Status	Confirmed By
Remote Code Execution (948590)		Based on the result of the "MS08-071: Vulnerabilities in GDI Could Allow Remote Code Execution" test, this node is vulnerable to this additional issue as well. C:\WINDOWS\system32\gdi32.dll has version 5.1.2600.2180 C:\WINDOWS\system32\gdi32.dll - file does exist
MS08-022: Vulnerability in VBScript and JScript Scripting Engines Could Allow Remote Code Execution (944338)	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 Based on the following 2 results: C:\WINDOWS\system32\vbscript.dll has version 5.6.0.8820 C:\WINDOWS\system32\vbscript.dll - file does exist C:\WINDOWS\system32\jscript.dll has version 5.6.0.8820
MS08-028: Vulnerability in Microsoft Jet Database Engine Could Allow Remote Code Execution (950749)	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 Based on the result of the "Windows XP Service Pack 3 (KB936929)" test, this node is vulnerable to this additional issue as well. C:\WINDOWS\system32\msxbde40.dll has version 4.0.8025.0 C:\WINDOWS\system32\msxbde40.dll - file does exist
MS08-030: Vulnerability in Bluetooth Stack Could Allow Remote Code Execution (951376)	Vulnerable Version	Vulnerable OS: Microsoft Windows XP Professional SP2 C:\WINDOWS\system32\drivers\bthport.sys has version 5.1.2600.2180 C:\WINDOWS\system32\drivers\bthport.sys has version 5.1.2600.2180
MS08-033: Vulnerabilities in DirectX Could Allow Remote Code Execution (951698)	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 Based on the result of the "MS09-011: Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution" test, this node is vulnerable to this additional

Name	Status	Confirmed By
		issue as well. C:\WINDOWS\system32\quartz.dll has version 6.5.2600.2180 C:\WINDOWS\system32\quartz.dll - file does exist HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WindowsCSDVersion - contains unexpected value 512
MS08-063: Vulnerability in SMB Could Allow Remote Code Execution	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 Based on the result of the "MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution" test, this node is vulnerable to this additional issue as well. C:\WINDOWS\system32\drivers\srv.sys has version 5.1.2600.2180 C:\WINDOWS\system32\drivers\srv.sys - file does exist HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WindowsCSDVersion - contains unexpected value 512
MS09-006: Vulnerabilities in Windows Kernel Could Allow Remote Code Execution	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 Based on the result of the "MS09-025: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege" test, this node is vulnerable to this additional issue as well. C:\WINDOWS\system32\win32k.sys has version 5.1.2600.2180 C:\WINDOWS\system32\win32k.sys - file does exist HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WindowsCSDVersion - contains unexpected value 512
MS09-022: Vulnerabilities in Windows Print Spooler Could Allow Remote Code Execution	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 C:\WINDOWS\system32\localspl.dll has version 5.1.2600.2180 C:\WINDOWS\system32\localspl.dll - file does exist

Name	Status	Confirmed By
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WindowsCSDVersion - contains unexpected value 512
MS09-025: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 C:\WINDOWS\system32\win32k.sys has version 5.1.2600.2180 C:\WINDOWS\system32\win32k.sys - file does exist HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WindowsCSDVersion - contains unexpected value 512
MS09-037: Vulnerabilities in Microsoft Active Template Library (ATL) Could Allow Remote Code Execution	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 C:\Program Files\Common Files\microsoft shared\triedit\dhtmled.ocx has version 6.1.0.9227 C:\Program Files\Common Files\microsoft shared\triedit\dhtmled.ocx - file does exist HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WindowsCSDVersion - contains unexpected value 512
MS09-038: Vulnerabilities in Windows Media File Processing Could Allow Remote Code Execution	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 C:\WINDOWS\system32\avifil32.dll has version 5.1.2600.2180 C:\WINDOWS\system32\avifil32.dll - file does exist HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WindowsCSDVersion - contains unexpected value 512
MS09-045: Vulnerability in JScript Scripting Engine Could Allow Remote Code Execution	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 Based on the following 2 results:Based on the following 3 results:C:\WINDOWS\system32\jscript.dll - file does exist

Name	Status	Confirmed By
		C:\WINDOWS\system32\jscript.dll has version 5.6.0.8820 C:\WINDOWS\system32\jscript.dll has version 5.6.0.8820 C:\WINDOWS\system32\jscript.dll has version 5.6.0.8820 C:\WINDOWS\system32\jscript.dll - file does exist
MS09-046: Vulnerability in DHTML Editing Component ActiveX Control Could Allow Remote Code Execution	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 C:\Program Files\Common Files\microsoft shared\triedit\triedit.dll has version 6.1.0.9227 C:\Program Files\Common Files\microsoft shared\triedit\triedit.dll - file does exist HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WindowsCSDVersion - contains unexpected value 512
MS09-047: Vulnerabilities in Windows Media Format Could Allow Remote Code Execution	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 Based on the following 2 results: C:\WINDOWS\system32\WMVCore.dll has version 9.0.0.3250 C:\WINDOWS\system32\WMVCore.dll has version 9.0.0.3250 C:\WINDOWS\system32\WMVCore.dll has version 9.0.0.3250 C:\WINDOWS\system32\WMVCore.dll has version 9.0.0.3250 C:\WINDOWS\system32\WMVCore.dll has version 9.0.0.3250 C:\WINDOWS\system32\WMVCore.dll has version 9.0.0.3250 Based on the following 2 results:

Name	Status	Confirmed By
		C:\WINDOWS\system32\WMVCore.dll has version 9.0.0.3250 C:\WINDOWS\system32\WMVCore.dll has version 9.0.0.3250
Multiple Mozilla Firefox Vulnerabilities Fixed in Version 2.0.0.12	Vulnerable Version	Vulnerable software installed: Mozilla Firefox 2.0.0.2
Multiple Mozilla Firefox Vulnerabilities: Fixed in 2.0.0.13	Vulnerable Version	Vulnerable software installed: Mozilla Firefox 2.0.0.2
Multiple Mozilla Firefox Vulnerabilities Fixed in version 2.0.0.15	Vulnerable Version	Vulnerable software installed: Mozilla Firefox 2.0.0.2
MS07-008: Vulnerability in HTML Help ActiveX Control Could Allow Remote Code Execution (928843)	Vulnerable Version	Vulnerable OS: Microsoft Windows XP Professional SP2 Based on the result of the "Windows XP Service Pack 3 (KB936929)" test, this node is vulnerable to this additional issue as well. Based on the following 2 results: C:\WINDOWS\system32\hhctrl.ocx - file does exist C:\WINDOWS\system32\hhctrl.ocx has version 5.2.3790.1194
MS07-008: Vulnerability in HTML Help ActiveX Control Could Allow Remote Code Execution (928843)	Vulnerable Version	Vulnerable OS: Microsoft Windows XP Professional SP2 Based on the result of the "Windows XP Service Pack 3 (KB936929)" test, this node is vulnerable to this additional issue as well. Based on the following 2 results: C:\WINDOWS\system32\hhctrl.ocx - file does exist C:\WINDOWS\system32\hhctrl.ocx has version 5.2.3790.1194
MS07-009: Vulnerability in Microsoft Data Access Components Could Allow Remote Code Execution (927779)	Vulnerable Version	Vulnerable OS: Microsoft Windows XP Professional SP2 Based on the result of the "Windows XP Service Pack 3 (KB936929)" test, this node is vulnerable to this additional issue as well. Based on the following 2 results:Based on the following 4

Name	Status	Confirmed By
		results:C:\Program Files\Common Files\System\ADO\msjro.dll has version 2.81.1117.0 C:\Program Files\Common Files\System\ADO\msadox.dll has version 2.81.1117.0 C:\Program Files\Common Files\System\ADO\msadomd.dll has version 2.81.1117.0 C:\Program Files\Common Files\System\ADO\msado15.dll has version 2.81.1117.0 C:\Program Files\Common Files\System\ADO\msjro.dll has version 2.81.1117.0
MS07-017: Vulnerability In GDI Could Allow Remote Code Execution (925902)	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 Based on the result of the "Windows XP Service Pack 3 (KB936929)" test, this node is vulnerable to this additional issue as well. C:\WINDOWS\system32\user32.dll has version 5.1.2600.2180 C:\WINDOWS\system32\user32.dll - file does exist
MS07-019: Vulnerability in Universal Plug and Play Could Allow Remote Code Execution (931261)	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 Based on the result of the "Windows XP Service Pack 3 (KB936929)" test, this node is vulnerable to this additional issue as well. C:\WINDOWS\system32\upnphost.dll has version 5.1.2600.2180 C:\WINDOWS\system32\upnphost.dll - file does exist
MS07-020: Vulnerability in Microsoft Agent Could Allow Remote Code Execution (932168)	Vulnerable Version	Vulnerable OS: Microsoft Windows XP Professional SP2 Based on the result of the "Windows XP Service Pack 3 (KB936929)" test, this node is vulnerable to this additional issue as well. C:\WINDOWS\system32\xpsp3res.dll - File not found: c:\windows\system32\xpsp3res.dll

Name	Status	Confirmed By
MS07-021: Vulnerability in CSRSS Could Allow Remote Code Execution (930178)	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 Based on the result of the "Windows XP Service Pack 3 (KB936929)" test, this node is vulnerable to this additional issue as well. C:\WINDOWS\system32\winsrv.dll has version 5.1.2600.2180 C:\WINDOWS\system32\winsrv.dll - file does exist
MS07-031: Vulnerability in the Windows Schannel Security Package Could Allow Remote Code Execution (935840)	Vulnerable Version	Vulnerable OS: Microsoft Windows XP Professional SP2 Based on the result of the "MS09-007: Vulnerability in SChannel Could Allow Spoofing" test, this node is vulnerable to this additional issue as well. Based on the following 2 results: C:\WINDOWS\system32\schannel.dll - file does exist C:\WINDOWS\system32\schannel.dll has version 5.1.2600.2180
MS07-031: Vulnerability in the Windows Schannel Security Package Could Allow Remote Code Execution (935840)	Vulnerable Version	Vulnerable OS: Microsoft Windows XP Professional SP2 Based on the result of the "MS09-007: Vulnerability in SChannel Could Allow Spoofing" test, this node is vulnerable to this additional issue as well. Based on the following 2 results: C:\WINDOWS\system32\schannel.dll - file does exist C:\WINDOWS\system32\schannel.dll has version 5.1.2600.2180
MS07-035: Vulnerability in Win 32 API Could Allow Remote Code Execution (935839)	Vulnerable Version	Vulnerable OS: Microsoft Windows XP Professional SP2 Based on the result of the "MS09-015: Blended Threat Vulnerability in SearchPath Could Allow Elevation of Privilege" test, this node is vulnerable to this additional issue as well. Based on the following 2 results: C:\WINDOWS\system32\kernel32.dll - file does exist C:\WINDOWS\system32\kernel32.dll has version 5.1.2600.2180

Name	Status	Confirmed By
MS07-042: Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution (936227)	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 Based on the result of the "MS08-069: Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution" test, this node is vulnerable to this additional issue as well. C:\WINDOWS\system32\msxml3.dll has version 8.50.2162.0 C:\WINDOWS\system32\msxml3.dll - file does exist
MS07-043: Vulnerability in OLE Automation Could Allow Remote Code Execution (921503)	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 Based on the result of the "MS08-008: Vulnerability in OLE Automation Could Allow Remote Code Execution (947890)" test, this node is vulnerable to this additional issue as well. C:\WINDOWS\system32\oleaut32.dll has version 5.1.2600.2180 C:\WINDOWS\system32\oleaut32.dll - file does exist
MS07-046: Vulnerability in GDI Could Allow Remote Code Execution (938829)	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 Based on the result of the "MS08-021: Vulnerabilities in GDI Could Allow Remote Code Execution (948590)" test, this node is vulnerable to this additional issue as well. C:\WINDOWS\system32\gdi32.dll has version 5.1.2600.2180 C:\WINDOWS\system32\gdi32.dll - file does exist
MS07-056: Security Update for Outlook Express and Windows Mail (941202)	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 Based on the result of the "MS08-048: Security Update for Outlook Express and Windows Mail (951066)" test, this node is vulnerable to this additional issue as well. Based on the following 2 results: C:\WINDOWS\system32\inetcomm.dll - file does exist C:\WINDOWS\system32\inetcomm.dll has version 6.0.2900.2180

Name	Status	Confirmed By
		C:\WINDOWS\system32\inetcomm.dll - file does exist
MS08-008: Vulnerability in OLE Automation Could Allow Remote Code Execution (947890)	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 Based on the result of the "Windows XP Service Pack 3 (KB936929)" test, this node is vulnerable to this additional issue as well. C:\WINDOWS\system32\oleaut32.dll has version 5.1.2600.2180 C:\WINDOWS\system32\oleaut32.dll - file does exist
MS08-068: Vulnerability in SMB Could Allow Remote Code Execution	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 C:\WINDOWS\system32\drivers\mrxsmb.sys has version 5.1.2600.2180 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WindowsCSDVersion - contains unexpected value 512
MS08-071: Vulnerabilities in GDI Could Allow Remote Code Execution	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 C:\WINDOWS\system32\gdi32.dll has version 5.1.2600.2180 C:\WINDOWS\system32\gdi32.dll - file does exist HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WindowsCSDVersion - contains unexpected value 512
MS08-076: Vulnerabilities in Windows Media Components Could Allow Remote Code Execution	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 C:\WINDOWS\system32\strmdll.dll has version 4.1.0.3928 C:\WINDOWS\system32\strmdll.dll - file does exist HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WindowsCSDVersion - contains unexpected value 512

Name	Status	Confirmed By
MS08-078: Security Update for Internet Explorer	Exploited	Vulnerable software installed: Microsoft Internet Explorer 6.0 SP2 Vulnerable OS: Microsoft Windows XP Professional SP2 Based on the result of the "MS09-014: Cumulative Security Update for Internet Explorer" test, this node is vulnerable to this additional issue as well. Based on the following 2 results:Based on the following 2 results:C:\Program Files\internet explorer\iexplore.exe has version 6.0.2900.2180 Based on the following 2 results: HKEY_LOCAL_MACHINE\SOFTWARE\microsoft\internet explorerVersion - contains 6.0.2900.2180 HKEY_LOCAL_MACHINE\SOFTWARE\microsoft\internet explorerVersion - contains 6.0.2900.2180 HKEY_LOCAL_MACHINE\SOFTWARE\microsoft\internet explorer\ActiveX Compatibility\Restriction Policies\Hashes\074ff50d0fbf0ccec37f65e137c91ee48442fe4c - key does not exist
MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 C:\WINDOWS\system32\drivers\srv.sys has version 5.1.2600.2180 C:\WINDOWS\system32\drivers\srv.sys - file does exist HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WindowsCSDVersion - contains unexpected value 512
MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution	Exploited	\BROWSER: WriteAndX succeeded with offset 77
MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution	Exploited	\BROWSER: WriteAndX succeeded with offset 77
MS09-007: Vulnerability in SChannel Could Allow Spoofing	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 C:\WINDOWS\system32\schannel.dll has version 5.1.2600.2180

Name	Status	Confirmed By
		C:\WINDOWS\system32\schannel.dll - file does exist HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WindowsCSDVersion - contains unexpected value 512
MS09-010: Vulnerabilities in WordPad and Office Text Converters Could Allow Remote Code Execution	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 Based on the following 2 results:C:\Program Files\windows nt\accessories\wordpad.exe has version 5.1.2600.2180 C:\Program Files\windows nt\accessories\wordpad.exe - file does exist HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WindowsCSDVersion - contains unexpected value 512 C:\WINDOWS\AppPatch\acadproc.dll - File not found: c:\windows\apppatch\acadproc.dll C:\Program Files\windows nt\accessories\mswrd8.wpc - file does exist
MS09-011: Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 Based on the result of the "MS09-028: Vulnerabilities in Microsoft DirectShow Could Allow Remote Code Execution" test, this node is vulnerable to this additional issue as well. C:\WINDOWS\system32\quartz.dll has version 6.5.2600.2180 C:\WINDOWS\system32\quartz.dll - file does exist HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WindowsCSDVersion - contains unexpected value 512
MS09-012: Vulnerabilities in Windows Could Allow Elevation of Privilege	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 C:\WINDOWS\system32\sc.exe has version 5.1.2600.0

Name	Status	Confirmed By
		C:\WINDOWS\system32\sc.exe - file does exist HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WindowsCSDVersion - contains unexpected value 512
MS09-013: Vulnerabilities in Windows HTTP Services Could Allow Remote Code Execution	Vulnerable Version	Vulnerable OS: Microsoft Windows XP Professional SP2 C:\WINDOWS\system32\winhttp.dll has version 5.1.2600.2180 C:\WINDOWS\system32\winhttp.dll has version 5.1.2600.2180
MS09-014: Cumulative Security Update for Internet Explorer	Exploited	Vulnerable software installed: Microsoft Internet Explorer 6.0 SP2 Vulnerable OS: Microsoft Windows XP Professional SP2 Based on the result of the "MS09-019: Cumulative Security Update for Internet Explorer" test, this node is vulnerable to this additional issue as well. Based on the following 2 results:Based on the following 2 results:C:\Program Files\internet explorer\iexplore.exe has version 6.0.2900.2180 Based on the following 2 results: HKEY_LOCAL_MACHINE\SOFTWARE\microsoft\internet explorerVersion - contains 6.0.2900.2180 HKEY_LOCAL_MACHINE\SOFTWARE\microsoft\internet explorerVersion - contains 6.0.2900.2180 HKEY_LOCAL_MACHINE\SOFTWARE\microsoft\internet explorer\ActiveX Compatibility\Restriction Policies\Hashes\074ff50d0fbf0ccec37f65e137c91ee48442fe4c - key does not exist
MS09-015: Blended Threat Vulnerability in SearchPath Could Allow Elevation of Privilege	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 C:\WINDOWS\system32\secur32.dll has version 5.1.2600.2180 C:\WINDOWS\system32\secur32.dll - file does exist

Name	Status	Confirmed By
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WindowsCSDVersion - contains unexpected value 512
MS09-019: Cumulative Security Update for Internet Explorer	Exploited	Vulnerable software installed: Microsoft Internet Explorer 6.0 SP2 Vulnerable OS: Microsoft Windows XP Professional SP2 Based on the result of the "MS09-034: Cumulative Security Update for Internet Explorer" test, this node is vulnerable to this additional issue as well. Based on the following 2 results:Based on the following 2 results:C:\Program Files\internet explorer\iexplore.exe has version 6.0.2900.2180 Based on the following 2 results: HKEY_LOCAL_MACHINE\SOFTWARE\microsoft\internet explorerVersion - contains 6.0.2900.2180 HKEY_LOCAL_MACHINE\SOFTWARE\microsoft\internet explorerVersion - contains 6.0.2900.2180 HKEY_LOCAL_MACHINE\SOFTWARE\microsoft\internet explorer\ActiveX Compatibility\Restriction Policies\Hashes\074ff50d0fbf0ccec37f65e137c91ee48442fe4c - key does not exist
MS09-026: Vulnerability in RPC Could Allow Elevation of Privilege	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 C:\WINDOWS\system32\rpcrt4.dll has version 5.1.2600.2180 C:\WINDOWS\system32\rpcrt4.dll - file does exist HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WindowsCSDVersion - contains unexpected value 512
MS09-028: Vulnerabilities in Microsoft DirectShow Could Allow Remote Code Execution	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 C:\WINDOWS\system32\quartz.dll has version 6.5.2600.2180

Name	Status	Confirmed By
		C:\WINDOWS\system32\quartz.dll - file does exist HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WindowsCSDVersion - contains unexpected value 512
MS09-029: Vulnerabilities in the Embedded OpenType Font Engine Could Allow Remote Code Execution	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 C:\WINDOWS\system32\t2embed.dll has version 0.2.0.81 C:\WINDOWS\system32\t2embed.dll - file does exist HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WindowsCSDVersion - contains unexpected value 512
MS09-032: Cumulative Security Update of ActiveX Kill Bits	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 HKEY_LOCAL_MACHINE\SOFTWARE\microsoft\internet explorer\ActiveX Compatibility\{22FD7C0A-850C-4A53-9821-0B0915C96139} - key does not exist
MS09-034: Cumulative Security Update for Internet Explorer	Exploited	Vulnerable software installed: Microsoft Internet Explorer 6.0 SP2 Vulnerable OS: Microsoft Windows XP Professional SP2 Based on the following 2 results:Based on the following 2 results:C:\Program Files\internet explorer\iexplore.exe has version 6.0.2900.2180 Based on the following 2 results: HKEY_LOCAL_MACHINE\SOFTWARE\microsoft\internet explorerVersion - contains 6.0.2900.2180 HKEY_LOCAL_MACHINE\SOFTWARE\microsoft\internet explorerVersion - contains 6.0.2900.2180 HKEY_LOCAL_MACHINE\SOFTWARE\microsoft\internet explorer\ActiveX Compatibility\Restriction Policies\Hashes\074ff50d0fbf0ccec37f65e137c91ee48442fe4c - key does not exist
MS09-040: Vulnerability in Message Queuing Could Allow Elevation of Privilege	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2

Name	Status	Confirmed By
		Based on the following 2 results:Based on the following 2 results:C:\WINDOWS\system32\mqrt.dll - file does exist HKEY_LOCAL_MACHINE\SOFTWARE\microsoft\MSMQ - key exists C:\WINDOWS\system32\mqutil.dll has version 5.1.0.1108 C:\WINDOWS\system32\mqutil.dll - file does exist
MS09-041: Vulnerability in Workstation Service Could Allow Elevation of Privilege	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 C:\WINDOWS\system32\wkssvc.dll has version 5.1.2600.2180 C:\WINDOWS\system32\wkssvc.dll - file does exist HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WindowsCSDVersion - contains unexpected value 512
Wireshark Multiple Vulnerabilities in NCP, zlib, Tektronix rf5 parsers	Vulnerable Version	Vulnerable software installed: The Wireshark developer community, http://www.wireshark.org Wireshark 0.99.6a

1.2.2. Severe Vulnerabilities

Name	Status	Confirmed By
CIFS Account Password Never Expires	Exploited	Password does not expire: user
CIFS Account Password Never Expires	Exploited	Password does not expire: user
CIFS Account Password Never Expires	Exploited	Password does not expire: Administrator
CIFS Account Password Never Expires	Exploited	Password does not expire: Administrator
MS08-061: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 Based on the result of the "MS09-006: Vulnerabilities in Windows Kernel Could Allow Remote Code Execution" test, this node is vulnerable to this additional issue as well. C:\WINDOWS\system32\win32k.sys has version 5.1.2600.2180 C:\WINDOWS\system32\win32k.sys - file does exist HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Co

Name	Status	Confirmed By
		ntrol\WindowsCSDVersion - contains unexpected value 512
MS08-066: Vulnerability in the Microsoft Ancillary Function Driver Could Allow Elevation of Privilege	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 Based on the following 2 results: C:\WINDOWS\system32\drivers\afd.sys has version 5.1.2600.2180 C:\WINDOWS\system32\drivers\afd.sys - file does exist HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WindowsCSDVersion - contains unexpected value 512 HKEY_LOCAL_MACHINE\SOFTWARE\Zone Labs\ZoneAlarm - key does not exist HKEY_LOCAL_MACHINE\SOFTWARE\Zone Labs\ZoneAlarm - key does not exist
MS08-069: Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 C:\WINDOWS\system32\msxml3.dll has version 8.50.2162.0 C:\WINDOWS\system32\msxml3.dll - file does exist HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WindowsCSDVersion - contains unexpected value 512
CIFS Account Lockout Policy Not Enforced	Vulnerable Version	Vulnerable OS: Microsoft Windows XP Professional SP2 The property "account-lockout-failure-threshold" contains: 0.
Office 2003 Service Pack 3 (SP3)	Exploited	Vulnerable software installed: Microsoft Office 2003 11.0.5614.0 Based on the following 2 results: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Products\9040111900063D11C8EF10054038389CVersion - contains unexpected value 184554990 HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\P

Name	Status	Confirmed By
		roducts\9040111900063D11C8EF10054038389C - key exists No patch with GUID {375F080F-88E9-4EA1-A177-C0F091546AC8} exists for the product. Based on the following 2 results: HKEY_LOCAL_MACHINE\SOFTWARE\microsoft\windows\currentversion\Installer\UserData\S-1-5-18\Products\9040111900063D11C8EF10054038389C\InstallProperties - key exists HKEY_LOCAL_MACHINE\SOFTWARE\microsoft\windows\currentversion\Installer\UserData\S-1-5-18\Products\9040111900063D11C8EF10054038389C\InstallPropertiesDisplayVersion - contains 11.0.5614.0
Windows XP Service Pack 3 (KB936929)	Vulnerable Version	Vulnerable OS: Microsoft Windows XP Professional SP2
Update Rollup for ActiveX Killbits for Windows XP (KB969898)	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 Based on the result of the "MS09-032: Cumulative Security Update of ActiveX Kill Bits" test, this node is vulnerable to this additional issue as well. HKEY_LOCAL_MACHINE\SOFTWARE\microsoft\internet explorer\ActiveX Compatibility\{22FD7C0A-850C-4A53-9821-0B0915C96139} - key does not exist
MS07-006: Vulnerability in Windows Shell Could Allow Elevation of Privilege (928255)	Vulnerable Version	Vulnerable OS: Microsoft Windows XP Professional SP2 Based on the result of the "Windows XP Service Pack 3 (KB936929)" test, this node is vulnerable to this additional issue as well. C:\WINDOWS\system32\shsvcs.dll has version 6.0.2900.2180 C:\WINDOWS\system32\shsvcs.dll - file does exist C:\WINDOWS\system32\xpsp3res.dll - File not found: c:\windows\system32\xpsp3res.dll
MS07-006: Vulnerability in Windows Shell Could Allow Elevation of Privilege (928255)	Vulnerable Version	Vulnerable OS: Microsoft Windows XP Professional SP2

Name	Status	Confirmed By
		Based on the result of the "Windows XP Service Pack 3 (KB936929)" test, this node is vulnerable to this additional issue as well. C:\WINDOWS\system32\shsvcs.dll has version 6.0.2900.2180 C:\WINDOWS\system32\shsvcs.dll - file does exist C:\WINDOWS\system32\xpsp3res.dll - File not found: c:\windows\system32\xpsp3res.dll
MS07-007: Vulnerability in Windows Image Acquisition Service Could Allow Elevation of Privilege (927802)	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 Based on the result of the "Windows XP Service Pack 3 (KB936929)" test, this node is vulnerable to this additional issue as well. C:\WINDOWS\system32\wiaservc.dll has version 5.1.2600.2180 C:\WINDOWS\system32\wiaservc.dll - file does exist
MS07-011: Vulnerability in Microsoft OLE Dialog Could Allow Remote Code Execution (926436)	Vulnerable Version	Vulnerable OS: Microsoft Windows XP Professional SP2 Based on the result of the "Windows XP Service Pack 3 (KB936929)" test, this node is vulnerable to this additional issue as well. Based on the following 2 results: C:\WINDOWS\system32\oledlg.dll - file does exist C:\WINDOWS\system32\oledlg.dll has version 5.1.2600.0
MS07-011: Vulnerability in Microsoft OLE Dialog Could Allow Remote Code Execution (926436)	Vulnerable Version	Vulnerable OS: Microsoft Windows XP Professional SP2 Based on the result of the "Windows XP Service Pack 3 (KB936929)" test, this node is vulnerable to this additional issue as well. Based on the following 2 results: C:\WINDOWS\system32\oledlg.dll - file does exist C:\WINDOWS\system32\oledlg.dll has version 5.1.2600.0
MS07-012: Vulnerability in Microsoft MFC	Vulnerable Version	Vulnerable OS: Microsoft Windows XP Professional SP2

Name	Status	Confirmed By
Could Allow Remote Code Execution (924667)		Based on the result of the "Windows XP Service Pack 3 (KB936929)" test, this node is vulnerable to this additional issue as well. Based on the following 2 results:Based on the following 2 results:C:\WINDOWS\system32\mfc42u.dll - file does exist C:\WINDOWS\system32\mfc40u.dll - file does exist C:\WINDOWS\system32\mfc42u.dll has version 6.2.4131.0
MS07-012: Vulnerability in Microsoft MFC Could Allow Remote Code Execution (924667)	Vulnerable Version	Vulnerable OS: Microsoft Windows XP Professional SP2 Based on the result of the "Windows XP Service Pack 3 (KB936929)" test, this node is vulnerable to this additional issue as well. Based on the following 2 results:Based on the following 2 results:C:\WINDOWS\system32\mfc42u.dll - file does exist C:\WINDOWS\system32\mfc40u.dll - file does exist C:\WINDOWS\system32\mfc42u.dll has version 6.2.4131.0
MS07-013: Vulnerability in Microsoft RichEdit Could Allow Remote Code Execution (918118)	Vulnerable Version	Vulnerable OS: Microsoft Windows XP Professional SP2 Based on the result of the "Windows XP Service Pack 3 (KB936929)" test, this node is vulnerable to this additional issue as well. Based on the following 2 results: C:\WINDOWS\system32\riched20.dll - file does exist C:\WINDOWS\system32\riched20.dll has version 5.30.23.1221
MS07-013: Vulnerability in Microsoft RichEdit Could Allow Remote Code Execution (918118)	Vulnerable Version	Vulnerable OS: Microsoft Windows XP Professional SP2 Based on the result of the "Windows XP Service Pack 3 (KB936929)" test, this node is vulnerable to this additional issue as well. Based on the following 2 results: C:\WINDOWS\system32\riched20.dll - file does exist C:\WINDOWS\system32\riched20.dll has version 5.30.23.1221

Name	Status	Confirmed By
MS07-022: Vulnerability in Windows Kernel Could Allow Elevation of Privilege (931784)	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 Based on the result of the "MS08-064: Vulnerability in Virtual Address Descriptor Manipulation Could Allow Elevation of Privilege" test, this node is vulnerable to this additional issue as well. C:\WINDOWS\system32\ntoskrnl.exe has version 5.1.2600.2180 C:\WINDOWS\system32\ntoskrnl.exe - file does exist
MS07-047: Vulnerabilities in Windows Media Player Could Allow Remote Code Execution (936782)	Vulnerable Version	Vulnerable OS: Microsoft Windows XP Professional SP2 Based on the result of the "MS09-037: Vulnerabilities in Microsoft Active Template Library (ATL) Could Allow Remote Code Execution" test, this node is vulnerable to this additional issue as well. Based on the following 2 results:Based on the following 2 results:C:\WINDOWS\system32\wmp.dll has version 9.0.0.3250 C:\WINDOWS\system32\wmp.dll has version 9.0.0.3250 C:\WINDOWS\system32\wmp.dll has version 9.0.0.3250 C:\WINDOWS\system32\wmp.dll has version 9.0.0.3250
MS07-058: Vulnerability in RPC Could Allow Denial of Service (933729)	Vulnerable Version	Vulnerable OS: Microsoft Windows XP Professional SP2 Based on the result of the "MS09-026: Vulnerability in RPC Could Allow Elevation of Privilege" test, this node is vulnerable to this additional issue as well. C:\WINDOWS\system32\xpsp3res.dll - File not found: c:\windows\system32\xpsp3res.dll
MS08-002: Vulnerability in LSASS Could Allow Local Elevation of Privilege (943485)	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 Based on the result of the "MS09-012: Vulnerabilities in Windows Could Allow Elevation of Privilege" test, this node

Name	Status	Confirmed By
		is vulnerable to this additional issue as well. C:\WINDOWS\system32\lsasrv.dll has version 5.1.2600.2180 C:\WINDOWS\system32\lsasrv.dll - file does exist
MS08-032: Cumulative Security Update of ActiveX Kill Bits (950760)	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 Based on the result of the "MS09-032: Cumulative Security Update of ActiveX Kill Bits" test, this node is vulnerable to this additional issue as well. HKEY_LOCAL_MACHINE\SOFTWARE\microsoft\internet explorer\ActiveX Compatibility\{22FD7C0A-850C-4A53-9821-0B0915C96139} - key does not exist
MS08-036: Vulnerabilities in Pragmatic General Multicast (PGM) Could Allow Denial of Service (950762)	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 C:\WINDOWS\system32\drivers\rmcast.sys has version 5.1.2600.0 C:\WINDOWS\system32\drivers\rmcast.sys - file does exist HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WindowsCSDVersion - contains unexpected value 512
MS08-049: Vulnerabilities in Event System Could Allow Remote Code Execution (950974)	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 C:\WINDOWS\system32\es.dll has version 2001.12.4414.258 C:\WINDOWS\system32\es.dll - file does exist HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WindowsCSDVersion - contains unexpected value 512
MS08-052: Vulnerabilities in GDI+ Could Allow Remote Code Execution (954593)	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 HKEY_LOCAL_MACHINE\SOFTWARE\microsoft\Windows NT\CurrentVersion\HotFix\KB938464 - key does not exist HKEY_LOCAL_MACHINE\SOFTWARE\microsoft\Windows NT\CurrentVersion\HotFix\KB938464-v2 - key does not exist

Name	Status	Confirmed By
MS08-064: Vulnerability in Virtual Address Descriptor Manipulation Could Allow Elevation of Privilege	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 Based on the result of the "MS09-012: Vulnerabilities in Windows Could Allow Elevation of Privilege" test, this node is vulnerable to this additional issue as well. C:\WINDOWS\system32\ntoskrnl.exe has version 5.1.2600.2180 C:\WINDOWS\system32\ntoskrnl.exe - file does exist HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WindowsCSDVersion - contains unexpected value 512
Wireshark Multiple Vulnerabilities in Bluetooth ACL, Q.931, Tamos CommView, USB, PRP and MATE dissectors	Vulnerable Version	Vulnerable software installed: The Wireshark developer community, http://www.wireshark.org Wireshark 0.99.6a
Wireshark NetScreen Snoop Capture File Buffer Overflow Vulnerability	Vulnerable Version	Vulnerable software installed: The Wireshark developer community, http://www.wireshark.org Wireshark 0.99.6a
Wireshark Vulnerability Fixed in version 1.0.8	Vulnerable Version	Vulnerable software installed: The Wireshark developer community, http://www.wireshark.org Wireshark 0.99.6a
Wireshark Multiple Vulnerabilities Fixed in version 1.2.1	Vulnerable Version	Vulnerable software installed: The Wireshark developer community, http://www.wireshark.org Wireshark 0.99.6a
Weak LAN Manager hashing permitted	Exploited	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LsaLMCompatibilityLevel - contains 0LMCompatibility - value does not exist
CIFS Minimum Password Length Policy Not Enforced	Vulnerable Version	Vulnerable OS: Microsoft Windows XP Professional SP2 The property "password-minimum-length" contains: 0.
Windows administrative shares enabled	Exploited	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServerStart - contains 2 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\ParametersAutoShareServer - value does not existAutoShareWks - value does not exist
Microsoft KB967940: Correct "Disable Autorun Registry Key" Enforcement	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 Based on the following 3 results: HKEY_LOCAL_MACHINE\SOFTWARE\microsoft\Windows NT\CurrentVersion\HotFix\KB950582 - key does not exist

Name	Status	Confirmed By
		Installed - value does not exist HKEY_LOCAL_MACHINE\SOFTWARE\microsoft\Windows NT\CurrentVersion\HotFix\KB953252 - key does not exist Installed - value does not exist HKEY_LOCAL_MACHINE\SOFTWARE\microsoft\Windows NT\CurrentVersion\HotFix\KB967715 - key does not exist Installed - value does not exist
MS07-034: Cumulative Security Update for Outlook Express and Windows Mail (929123)	Vulnerable Version	Vulnerable OS: Microsoft Windows XP Professional SP2 Based on the result of the "Windows XP Service Pack 3 (KB936929)" test, this node is vulnerable to this additional issue as well. Based on the following 2 results:Based on the following 5 results:C:\WINDOWS\system32\inetcomm.dll - file does exist C:\Program Files\Common Files\SYSTEM\wab32.dll - file does exist C:\Program Files\Common Files\SYSTEM\directdb.dll - file does exist C:\Program Files\Outlook Express\wabimp.dll - file does exist C:\Program Files\Outlook Express\msoe.dll - file does exist C:\WINDOWS\system32\inetcomm.dll has version 6.0.2900.2180
MS07-034: Cumulative Security Update for Outlook Express and Windows Mail (929123)	Vulnerable Version	Vulnerable OS: Microsoft Windows XP Professional SP2 Based on the result of the "Windows XP Service Pack 3 (KB936929)" test, this node is vulnerable to this additional issue as well. Based on the following 2 results:Based on the following 5 results:C:\WINDOWS\system32\inetcomm.dll - file does exist C:\Program Files\Common Files\SYSTEM\wab32.dll - file does exist C:\Program Files\Common Files\SYSTEM\directdb.dll - file does exist C:\Program Files\Outlook Express\wabimp.dll - file does exist C:\Program Files\Outlook Express\msoe.dll - file does exist C:\WINDOWS\system32\inetcomm.dll has version

Name	Status	Confirmed By
		6.0.2900.2180
MS07-050: Vulnerability in Vector Markup Language Could Allow Remote Code Execution (938127)	Vulnerable Version	Vulnerable OS: Microsoft Windows XP Professional SP2 Based on the result of the "Windows XP Service Pack 3 (KB936929)" test, this node is vulnerable to this additional issue as well. Based on the following 2 results:Based on the following 2 results:C:\Program Files\Common Files\microsoft shared\vgx\vgx.dll - file does exist C:\Program Files\internet explorer\iexplore.exe has version 6.0.2900.2180 C:\Program Files\Common Files\microsoft shared\vgx\vgx.dll has version 6.0.2900.2180
MS07-050: Vulnerability in Vector Markup Language Could Allow Remote Code Execution (938127)	Vulnerable Version	Vulnerable OS: Microsoft Windows XP Professional SP2 Based on the result of the "Windows XP Service Pack 3 (KB936929)" test, this node is vulnerable to this additional issue as well. Based on the following 2 results:Based on the following 2 results:C:\Program Files\Common Files\microsoft shared\vgx\vgx.dll - file does exist C:\Program Files\internet explorer\iexplore.exe has version 6.0.2900.2180 C:\Program Files\Common Files\microsoft shared\vgx\vgx.dll has version 6.0.2900.2180
MS07-068: Vulnerability in Windows Media File Format Could Allow Remote Code Execution (941569 and 944275)	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 Based on the result of the "Windows XP Service Pack 3 (KB936929)" test, this node is vulnerable to this additional issue as well. Based on the following 2 results: C:\WINDOWS\system32\wmasf.dll has version 9.0.0.3250 C:\WINDOWS\system32\wmasf.dll has version 9.0.0.3250

Name	Status	Confirmed By
		Based on the following 3 results: C:\WINDOWS\system32\wmasf.dll - file does exist C:\WINDOWS\system32\wmasf.dll has version 9.0.0.3250 C:\WINDOWS\system32\wmasf.dll has version 9.0.0.3250
MS08-048: Security Update for Outlook Express and Windows Mail (951066)	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 C:\WINDOWS\system32\inetcomm.dll has version 6.0.2900.2180 C:\WINDOWS\system32\inetcomm.dll - file does exist HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WindowsCSDVersion - contains unexpected value 512
Windows security policy violation	Exploited	There were 3 policy violations for the "Default Security Settings. User Rights\Restricted Groups not included. (Windows 2000 Professional)" security policy.
Wireshark DoS Vulnerabilities in SCCP, LDAP, Roofnet, X509sat Dissectors	Vulnerable Version	Vulnerable software installed: The Wireshark developer community, http://www.wireshark.org Wireshark 0.99.6a
Wireshark DoS Vulnerabilities in SCTP, SNMP, TFTP Dissectors	Vulnerable Version	Vulnerable software installed: The Wireshark developer community, http://www.wireshark.org Wireshark 0.99.6a
Windows display last username enabled	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 HKEY_LOCAL_MACHINE\SOFTWARE\microsoft\windows\currentversion\Policies\SystemDontDisplayLastUserName - contains unexpected value 0
MS07-065: Vulnerability in Message Queuing Could Allow Remote Code Execution (937894)	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 Based on the result of the "MS09-040: Vulnerability in Message Queuing Could Allow Elevation of Privilege" test, this node is vulnerable to this additional issue as well. C:\WINDOWS\system32\mqutil.dll has version 5.1.0.1108 C:\WINDOWS\system32\mqutil.dll - file does exist

Name	Status	Confirmed By
MS08-020: Vulnerability in DNS Client Could Allow Spoofing (945553)	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 Based on the result of the "Windows XP Service Pack 3 (KB936929)" test, this node is vulnerable to this additional issue as well. C:\WINDOWS\system32\dnsrslvr.dll has version 5.1.2600.2180 C:\WINDOWS\system32\dnsrslvr.dll - file does exist
MS08-025: Vulnerability in Windows Kernel Could Allow Elevation of Privilege (941693)	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 Based on the result of the "MS08-061: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege" test, this node is vulnerable to this additional issue as well. C:\WINDOWS\system32\win32k.sys has version 5.1.2600.2180 C:\WINDOWS\system32\win32k.sys - file does exist
MS08-050: Vulnerability in Windows Messenger Could Allow Information Disclosure (955702)	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 Based on the following 2 results:Based on the following 3 results:C:\Program Files\Messenger\msgsc.dll - file does exist C:\Program Files\Messenger\msgsc.dll has version 4.7.0.3000 C:\Program Files\Messenger\msgsc.dll has version 4.7.0.3000 C:\Program Files\messenger\msgsc.dll has version 4.7.0.3000 C:\Program Files\messenger\msgsc.dll - file does exist HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WindowsCSDVersion - contains unexpected value 512
Printer driver installation is not restricted	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2

Name	Status	Confirmed By
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print\Providers\LanMan Print Services\Servers AddPrinterDrivers - contains 0

1.2.3. Moderate Vulnerabilities

Name	Status	Confirmed By
Wireshark Multiple Vulnerabilities in GSM SMS, PANA, KISMET, RTMPT, RMI, SS7 MSU	Vulnerable Version	Vulnerable software installed: The Wireshark developer community, http://www.wireshark.org Wireshark 0.99.6a
Wireshark Packet Reassembly Denial of Service	Vulnerable Version	Vulnerable software installed: The Wireshark developer community, http://www.wireshark.org Wireshark 0.99.6a
CIFS NULL Session Permitted	Exploited	Found server name: IML-DESKTOP2
Windows XP firewall settings are unsafe	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfileDisableNotifications - value does not exist EnableFirewall - contains unexpected value 0 DoNotAllowExceptions - value does not exist
Windows XP Security Center settings are unsafe	Exploited	Vulnerable OS: Microsoft Windows XP Professional SP2 HKEY_LOCAL_MACHINE\SOFTWARE\microsoft\Security CenterAntiVirusDisableNotify - contains unexpected value 1FirewallDisableNotify - contains unexpected value 1 AntiVirusOverride - contains 0FirewallOveride - value does not exist