Nessus Report

Report

24/Feb/2012:17:48:13 GMT

Table Of Contents

Hosts Summary (Executive)

192.168.1.205

Summary

Critical	High	Medium	Low	Info	Total
31	152	39	4	29	255

Details

Severity	Plugin Id	Name
Critical (10.0)	11790	MS03-026 / MS03-039: Buffer Overrun In RPCSS Service Could Allow Code Execution (823980 / 824146)
Critical (10.0)	11808	MS03-026: Microsoft RPC Interface Buffer Overrun (823980)
Critical (10.0)	11835	MS03-039: Microsoft RPC Interface Buffer Overrun (824146) (uncredentialed check)
Critical (10.0)	11888	MS03-043: Buffer Overrun in Messenger Service (828035)
Critical (10.0)	11921	MS03-049: Buffer Overflow in the Workstation Service (828749)
Critical (10.0)	12052	MS04-007: ASN.1 parsing vulnerability (828028)
Critical (10.0)	12205	MS04-011: Microsoft Hotfix (credentialed check) (835732)
Critical (10.0)	12206	MS04-012: Microsoft Hotfix (credentialed check) (828741)
Critical (10.0)	15456	MS04-031: Vulnerability in NetDDE Could Allow Code Execution (841533)
Critical (10.0)	18483	MS05-027: Vulnerability in SMB Could Allow Remote Code Execution (896422)
Critical (10.0)	18502	MS05-027: Vulnerability in SMB Could Allow Remote Code Execution (896422) (uncredentialed check)
Critical (10.0)	19402	MS05-039: Vulnerability in Plug and Play Could Allow Remote Code Execution and Elevation of Privilege (899588)
Critical (10.0)	19406	MS05-043: Vulnerability in Print Spooler Service Could Allow Remote Code Execution (896423)
Critical (10.0)	19407	MS05-043: Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423) (uncredentialed check)
Critical (10.0)	19408	MS05-039: Vulnerability in Plug and Play Service Could Allow Remote Code Execution (899588) (uncredentialed check)
Critical (10.0)	19999	MS05-046: Vulnerability in the Client Service for NetWare Could Allow Remote Code Execution (899589)
Critical (10.0)	20004	MS05-051: Vulnerabilities in MSDTC and COM+ Could Allow Remote Code Execution (902400)
Critical (10.0)	21193	MS05-047: Plug and Play Remote Code Execution and Local Privilege Elevation (905749) (uncredentialed check)
Critical (10.0)	21692	MS06-030: Vulnerability in Server Message Block Could Allow Elevation of Privilege (914389)
Critical (10.0)	22182	MS06-040: Vulnerability in Server Service Could Allow Remote Code Execution (921883)

Critical (10.0)	22183	MS06-041: Vulnerability in DNS Resolution Could Allow Remote Code Execution (920683)
Critical (10.0)	22194	MS06-040: Vulnerability in Server Service Could Allow Remote Code Execution (921883) (uncredentialed check)
Critical (10.0)	23646	MS06-070: Vulnerability in Workstation Service Could Allow Remote Code Execution (924270)
Critical (10.0)	24340	MS07-016: Cumulative Security Update for Internet Explorer (928090)
Critical (10.0)	29893	MS08-001: Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (941644)
Critical (10.0)	34476	MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Unspecified Remote Code Execution (958644)
Critical (10.0)	35361	MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (958687)
Critical (10.0)	39344	MS09-022: Vulnerabilities in Windows Print Spooler Could Allow Remote Code Execution (961501)
Critical (10.0)	39348	MS09-026: Vulnerability in RPC Could Allow Elevation of Privilege (970238)
Critical (10.0)	43063	MS09-071: Vulnerabilities in Internet Authentication Service Could Allow Remote Code Execution (974318)
Critical (10.0)	44422	MS10-012: Vulnerabilities in SMB Could Allow Remote Code Execution (971468)
High (9.3)	10861	MS02-005: MSIE 5.01 5.5 6.0 Cumulative Patch (890923)
High (9.3)	11878	MS03-023: Buffer Overrun In HTML Converter Could Allow Code Execution (823559)
High (9.3)	11887	MS03-042: Buffer Overflow in Windows Troubleshooter ActiveX Control (826232)
High (9.3)	11928	MS03-044: Buffer Overrun in Windows Help (825119)
High (9.3)	13642	MS04-024: Buffer overrun in Windows Shell (839645)
High (9.3)	15457	MS04-032: Security Update for Microsoft Windows (840987)
High (9.3)	15460	MS04-037: Vulnerability in Windows Shell (841356)
High (9.3)	16123	MS05-001: HTML Help Code Execution (890175)
High (9.3)	16124	MS05-002: Cursor and Icon Format Handling Code Execution (891711)
High (9.3)	16324	MS05-008: Vulnerability in Windows Shell (890047)
High (9.3)	16326	MS05-011: Vulnerability in SMB may allow remote code execution (885250)
High (9.3)	16329	MS05-013: Vulnerability in the DHTML Editing Component may allow code execution (891781)
High (9.3)	18215	MS05-024: Vulnerability in Web View Could Allow Code Execution (894320)
High (9.3)	18482	MS05-026: Vulnerability in HTML Help Could Allow Remote Code Execution (896358)

High (9.3)	18490	MS05-025: Cumulative Security Update for Internet Explorer (883939)
High (9.3)	18681	MS05-036: Vulnerability in Microsoft Color Management Module Could Allow Remote Code Execution (901214)
High (9.3)	19401	MS05-038: Cumulative Security Update for Internet Explorer (896727)
High (9.3)	20003	MS05-050: Vulnerability in DirectShow Could Allow Remote Code Execution (904706)
High (9.3)	20005	MS05-052: Cumulative Security Update for Internet Explorer (896688)
High (9.3)	20906	MS06-006: Vulnerability in Windows Media Player Plug-in Could Allow Remote Code Execution (911564)
High (9.3)	21210	MS06-013: Cumulative Security Update for Internet Explorer (912812)
High (9.3)	22449	MS06-055: Vulnerability in Vector Markup Language Could Allow Remote Code Execution (925486)
High (9.3)	22530	MS06-057: Vulnerability in Windows Explorer Could Allow Remote Execution (923191)
High (9.3)	23833	MS06-072: Cumulative Security Update for Internet Explorer (925454)
High (9.3)	24000	MS07-004: Vulnerability in Vector Markup Language Could Allow Remote Code Execution (929969)
High (9.3)	24332	MS07-008: Vulnerability in HTML Help ActiveX Control Could Allow Remote Code Execution (928843)
High (9.3)	24333	MS07-009: Vulnerability in Microsoft Data Access Components Could Allow Remote Code Execution (927779)
High (9.3)	24336	MS07-012: Vulnerability in Microsoft MFC Could Allow Remote Code Execution (924667)
High (9.3)	24337	MS07-013: Vulnerability in Microsoft RichEdit Could Allow Remote Code Execution (918118)
High (9.3)	24911	MS07-017: Vulnerabilities in GDI Could Allow Remote Code Execution (925902)
High (9.3)	25023	MS07-020: Vulnerability in Microsoft Agent Could Allow Remote Code Execution (932168)
High (9.3)	25024	MS07-021: Vulnerabilities in CSRSS Could Allow Remote Code Execution (930178)
High (9.3)	25166	MS07-027: Cumulative Security Update for Internet Explorer (931768)
High (9.3)	25484	MS07-031: Vulnerability in the Windows Schannel Security Package Could Allow Remote Code Execution (935840)
High (9.3)	25486	MS07-033: Cumulative Security Update for Internet Explorer (933566)
High (9.3)	25488	MS07-035: Vulnerability in Win 32 API Could Allow Remote Code Execution (935839)
High (9.3)	25881	MS07-043: Vulnerability in OLE Automation Could Allow Remote Code Execution (921503)
High (9.3)	25883	MS07-045: Cumulative Security Update for Internet Explorer (937143)

High (9.3)	25884	MS07-046: Vulnerability in GDI Could Allow Remote Code Execution (938829)
High (9.3)	25886	MS07-050: Vulnerability in Vector Markup Language Could Allow Remote Code Execution (938127)
High (9.3)	26017	MS07-051: Vulnerability in Microsoft Agent Could Allow Remote Code Execution (938827)
High (9.3)	26961	MS07-055: Vulnerability in Kodak Image Viewer Could Allow Remote Code Execution (923810)
High (9.3)	26962	MS07-056: Cumulative Security Update for Outlook Express and Windows Mail (941202)
High (9.3)	26963	MS07-057: Cumulative Security Update for Internet Explorer (939653)
High (9.3)	29308	MS07-064: Vulnerabilities in DirectX Could Allow Remote Code Execution (941568)
High (9.3)	29313	MS07-069: Cumulative Security Update for Internet Explorer (942615)
High (9.3)	31042	MS08-008: Vulnerability in OLE Automation Could Allow Remote Code Execution (947890)
High (9.3)	31044	MS08-010: Cumulative Security Update for Internet Explorer (944533)
High (9.3)	31794	MS08-021: Vulnerabilities in GDI Could Allow Remote Code Execution (948590)
High (9.3)	31797	MS08-024: Cumulative Security Update for Internet Explorer (947864)
High (9.3)	32312	MS08-028: Vulnerability in Microsoft Jet Database Engine Could Allow Remote Code Execution (950749)
High (9.3)	33133	MS08-031: Cumulative Security Update for Internet Explorer (950759)
High (9.3)	33135	MS08-033: Vulnerabilities in DirectX Could Allow Remote Code Execution (951698)
High (9.3)	33874	MS08-045: Cumulative Security Update for Internet Explorer (953838)
High (9.3)	33875	MS08-046: Vulnerability in Microsoft Windows Image Color Management System Could Allow Remote Code Execution (952954)
High (9.3)	34403	MS08-058: Microsoft Internet Explorer Multiple Vulnerabilities (956390)
High (9.3)	35070	MS08-071: Vulnerabilities in GDI+ Could Allow Remote Code Execution (956802)
High (9.3)	35072	MS08-073: Microsoft Internet Explorer Multiple Vulnerabilities (958215)
High (9.3)	35221	MS08-078: Microsoft Internet Explorer Security Update (960714)
High (9.3)	35822	MS09-006: Vulnerabilities in Windows Kernel Could Allow Remote Code Execution (958690)
High (9.3)	35823	MS09-007: Vulnerability in SChannel Could Allow Spoofing (960225)
High (9.3)	36151	MS09-013: Vulnerabilities in Windows HTTP Services Could Allow Remote Code Execution (960803)
High (9.3)	36152	MS09-014: Cumulative Security Update for Internet Explorer (963027)

High (9.3)	36153	MS09-015: Blended Threat Vulnerability in SearchPath Could Allow Elevation of Privilege (959426)
High (9.3)	39341	MS09-019: Cumulative Security Update for Internet Explorer (969897)
High (9.3)	39791	MS09-028: Vulnerabilities in Microsoft DirectShow Could Allow Remote Code Execution (971633)
High (9.3)	39792	MS09-029: Vulnerabilities in the Embedded OpenType Font Engine Could Allow Remote Code Execution (961371)
High (9.3)	40407	MS09-034: Cumulative Security Update for Internet Explorer (972260)
High (9.3)	40556	MS09-037: Vulnerabilities in Microsoft Active Template Library (ATL) Could Allow Remote Code Execution (973908)
High (9.3)	40557	MS09-038: Vulnerabilities in Windows Media File Processing Could Allow Remote Code Execution (971557)
High (9.3)	40561	MS09-042: Vulnerability in Telnet Could Allow Remote Code Execution (960859)
High (9.3)	40888	MS09-045: Vulnerability in JScript Scripting Engine Could Allow Remote Code Execution (971961)
High (9.3)	40889	MS09-046: Vulnerability in DHTML Editing Component ActiveX Control Could Allow Remote Code Execution (956844)
High (9.3)	42110	MS09-054: Cumulative Security Update for Internet Explorer (974455)
High (9.3)	42439	MS09-065: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (969947)
High (9.3)	43064	MS09-072: Cumulative Security Update for Internet Explorer (976325)
High (9.3)	43065	MS09-073: Vulnerability in WordPad and Office Text Converters Could Allow Remote Code Execution (975539)
High (9.3)	43089	MS KB955759: Security Enhancements for the Indeo Codec
High (9.3)	43865	MS10-001: Vulnerability in the Embedded OpenType Font Engine Could Allow Remote Code Execution (972270)
High (9.3)	44110	MS10-002: Cumulative Security Update for Internet Explorer (978207)
High (9.3)	44417	MS10-007: Vulnerability in Windows Shell Handler Could Allow Remote Code Execution (975713)
High (9.3)	44423	MS10-013: Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution (977935)
High (9.3)	45378	MS10-018: Cumulative Security Update for Internet Explorer (980182)
High (9.3)	45506	MS10-019: Vulnerabilities in Windows Could Allow Remote Code Execution (981210)
High (9.3)	45507	MS10-020: Vulnerabilities in SMB Client Could Allow Remote Code Execution (980232)
High (9.3)	45513	MS10-026: Vulnerability in Microsoft MPEG Layer-3 Codecs Could Allow Remote Code Execution (977816)

High (9.3)	46312	MS10-030: Vulnerability in Outlook Express and Windows Mail Could Allow Remote Code Execution (978542)
High (9.3)	46840	MS10-033: Vulnerabilities in Media Decompression Could Allow Remote Code Execution (979902)
High (9.3)	46842	MS10-035: Cumulative Security Update for Internet Explorer (982381)
High (9.3)	48762	MS KB2269637: Insecure Library Loading Could Allow Remote Code Execution
High (9.0)	18023	MS05-019: Vulnerabilities in TCP/IP Could Allow Remote Code Execution (893066)
High (9.0)	20000	MS05-047: Vulnerability in Plug and Play Could Allow Remote Code Execution and Local Elevation of Privilege (905749)
High (9.0)	34408	MS08-063: Microsoft Windows SMB File Name Handling Remote Underflow (957095)
High (9.0)	42109	MS09-053: Vulnerabilities in FTP Service for Internet Information Services Could Allow Remote Code Execution (975254)
High (8.5)	33878	MS08-049: Vulnerabilities in Event System Could Allow Remote Code Execution (950974)
High (7.8)	26964	MS07-058: Vulnerability in RPC Could Allow Denial of Service (933729)
High (7.6)	11301	MS02-040 / MS03-033: Unchecked buffer in MDAC Function (326573 / 823718)
High (7.6)	11886	MS03-041: Vulnerability in Authenticode Verification Could Allow Remote Code Execution (823182)
High (7.6)	12207	MS04-014: Microsoft Hotfix (credentialed check) (837001)
High (7.6)	13640	MS04-022: Task Scheduler Vulnerability (841873)
High (7.6)	13641	MS04-023: Vulnerability in HTML Help Could Allow Code Execution (840315)
High (7.6)	15964	MS04-043: Vulnerabilities in HyperTerminal (873339)
High (7.6)	15966	MS04-041: Vulnerabilities in WordPad (885836)
High (7.6)	16125	MS05-003: Indexing Service Code Execution (871250)
High (7.6)	16327	MS05-012: Vulnerability in OLE and COM Could Allow Code Execution (873333)
High (7.6)	16330	MS05-015: Vulnerability in the Hyperlink Object Library may allow code execution (888113)
High (7.6)	18020	MS05-016: Vulnerability in Windows Shell (893086)
High (7.6)	18489	MS05-030: Vulnerability in Outlook Express Could Allow Remote Code Execution (897715)
High (7.6)	20001	MS05-048: Vulnerability in the Microsoft Collaboration Data Objects Could Allow Remote Code Execution (907245)
High (7.6)	20002	MS05-049: Vulnerabilities in Windows Shell Could Allow Remote Code Execution (900725)

High (7.6)	20172	MS05-053: Vulnerabilities in Graphics Rendering Engine Could Allow Code Execution (896424)
High (7.6)	23644	MS06-067: Cumulative Security Update for Internet Explorer (922760)
High (7.6)	24335	MS07-011: Vulnerability in Microsoft OLE Dialog Could Allow Remote Code Execution (926436)
High (7.6)	34743	MS08-068: Vulnerability in SMB Could Allow Remote Code Execution (957097)
High (7.6)	42113	MS09-057: Vulnerability in Indexing Service Could Allow Remote Code Execution (969059)
High (7.6)	42114	MS09-058: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (971486)
High (7.6)	44415	MS10-005: Vulnerability in Microsoft Paint Could Allow Remote Code Execution (978706)
High (7.6)	44416	MS10-006: Vulnerabilities in SMB Client Could Allow Remote Code Execution (978251)
High (7.6)	45509	MS10-022: Vulnerability in VBScript Scripting Engine Could Allow Remote Code Execution (981169)
High (7.5)	20299	MS05-054: Cumulative Security Update for Internet Explorer (905915)
High (7.5)	20382	MS06-001: Vulnerabilities in Graphics Rendering Engine Could Allow Code Execution (912919)
High (7.5)	20389	MS06-002: Vulnerability in Embedded Web Fonts Could Allow Remote Code Execution (908519)
High (7.5)	21331	MS06-018: Vulnerability in MSDTC Could Allow Denial of Service (913580)
High (7.5)	21685	MS06-021: Cumulative Security Update for Internet Explorer (916281)
High (7.5)	21689	MS06-025: Vulnerability in Routing and Remote Access Could Allow Remote Code Execution (911280)
High (7.5)	21694	MS06-032: Vulnerability in TCP/IP Could Allow Remote Code Execution (917953)
High (7.5)	22029	MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution (917159)
High (7.5)	22030	MS06-036: Vulnerability in DHCP Client Service Could Allow Remote Code Execution (914388)
High (7.5)	22034	MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution (917159) (uncredentialed check)
High (7.5)	22184	MS06-042: Cumulative Security Update for Internet Explorer (918899)
High (7.5)	22188	MS06-046: Vulnerability in HTML Help Could Allow Remote Code Execution (922616)
High (7.5)	22191	MS06-049: Vulnerability in Windows Kernel Could Result in Elevation of Privilege (920958)
High (7.5)	22192	MS06-050: Vulnerabilities in Microsoft Windows Hyperlink Object Library Could Allow Remote Code Execution (920670)

High (7.5)	22193	MS06-051: Vulnerability in Windows Kernel Could Result in Remote Code Execution (917422)
High (7.5)	22536	MS06-063: Vulnerability in Server Service Could Allow Denial of Service (923414)
High (7.5)	23643	MS06-066: Vulnerability in the Client Service for NetWare Could Allow Remote Code Execution (923980)
High (7.5)	23645	MS06-068: Vulnerability in Microsoft Agent Could Remote Code Execution (920213)
High (7.5)	23838	MS06-078: Vulnerability in Windows Media Format Could Allow Remote Code Execution (923689/925398)
High (7.5)	35075	MS08-076: Vulnerabilities in Windows Media Components Could Allow Remote Code Execution (959807)
High (7.5)	39342	MS09-020: Vulnerabilities in Internet Information Services (IIS) Could Allow Elevation of Privilege (970483)
High (7.2)	11885	MS03-045: Buffer Overrun in the ListBox and in the ComboBox (824141)
High (7.2)	13637	MS04-019: Utility Manager Could Allow Code Execution (842526)
High (7.2)	15963	MS04-044: Vulnerabilities in Windows Kernel and LSASS (885835)
High (7.2)	19403	MS05-040: Vulnerability in Telephony Service Could Allow Remote Code Execution (893756)
High (7.2)	20298	MS05-055: Vulnerability in Windows Kernel Could Allow Elevation of Privilege (908523)
High (7.2)	25025	MS07-022: Vulnerability in Windows Kernel Could Allow Elevation of Privilege (931784)
High (7.2)	29894	MS08-002: Vulnerability in LSASS Could Allow Local Elevation of Privilege (943485)
High (7.2)	31798	MS08-025: Vulnerability in Windows Kernel Could Allow Elevation of Privilege (941693)
High (7.2)	34406	MS08-061: Microsoft Windows Kernel Multiple Privilege Elevation (954211)
High (7.2)	36150	MS09-012: Vulnerabilities in Windows Could Allow Elevation of Privilege (959454)
High (7.2)	39347	MS09-025: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (968537)
High (7.2)	46839	MS10-032: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (979559)
Medium (6.9)	44421	MS10-011: Vulnerability in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege (978037)
Medium (6.9)	46844	MS10-037: Vulnerability in the OpenType Compact Font Format (CFF) Driver Could Allow Elevation of Privilege (980218)
Medium (6.8)	11990	MS04-003: MDAC Buffer Overflow (832483)
Medium (6.8)	21687	MS06-023: Vulnerability in Microsoft JScript Could Allow Remote Code Execution (917344)

Medium (6.8)	23835	MS06-076: Cumulative Security Update for Outlook Express (923694)
Medium (6.8)	31039	MS08-005: Vulnerability in Internet Information Services Could Allow Elevation of Privilege (942831)
Medium (6.8)	43061	MS09-069: Vulnerability in Local Security Authority Subsystem Service Could Allow Denial of Service (974392)
Medium (6.8)	52977	MS KB2524375: Fraudulent Digital Certificates Could Allow Spoofing
Medium (6.5)	22028	MS06-034: Vulnerability in Microsoft IIS using ASP Could Allow Remote Code Execution (917537)
Medium (6.4)	45511	MS10-024: Vulnerabilities in Microsoft Exchange and Windows SMTP Service Could Allow Denial of Service (981832)
Medium (6.2)	44425	MS10-015: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (977165)
Medium (6.2)	45508	MS10-021: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (979683)
Medium (6.0)	22186	MS06-044: Vulnerability in Microsoft Management Console Could Allow Remote Code Execution (917008)
Medium (5.8)	31793	MS08-020: Vulnerability in DNS Client Could Allow Spoofing (945553)
Medium (5.8)	33441	MS08-037: Vulnerabilities in DNS Could Allow Spoofing (953230)
Medium (5.4)	33877	MS08-048: Security Update for Outlook Express and Windows Mail (951066)
Medium (5.1)	18592	Microsoft Windows 2000 SP4 Update Rollup 1 Missing
Medium (5.1)	21211	MS06-014: Vulnerability in MDAC Could Allow Code Execution (911562)
Medium (5.1)	21212	MS06-015: Vulnerabilities in Windows Explorer Could Allow Remote Code Execution (908531)
Medium (5.1)	21213	MS06-016: Vulnerability in Outlook Express Could Allow Remote Code Execution (911567)
Medium (5.1)	22187	MS06-045: Vulnerability in Windows Explorer Could Allow Remote Code Execution (921398)
Medium (5.1)	33134	MS08-032: Cumulative Security Update of ActiveX Kill Bits (950760)
Medium (5.1)	33881	MS KB953839: Cumulative Security Update of ActiveX Kill Bits
Medium (5.1)	34414	MS KB956391: Cumulative Security Update of ActiveX Kill Bits
Medium (5.1)	35634	MS KB960715: Cumulative Security Update of ActiveX Kill Bits
Medium (5.1)	39350	MS KB969898: Cumulative Security Update of ActiveX Kill Bits
Medium (5.1)	39622	MS09-032: Cumulative Security Update of ActiveX Kill Bits (973346)
Medium (5.1)	42111	MS09-055: Cumulative Security Update of ActiveX Kill Bits (973525)
Medium (5.1)	44418	MS10-008: Cumulative Security Update of ActiveX Kill Bits (978262)
Medium (5.1)	46841	MS10-034: Cumulative Security Update of ActiveX Kill Bits (980195)

Medium (5.0)	12267	MS04-016: Vulnerability in DirectPlay Could Allow Denial of Service (839643)
Medium (5.0)	18585	Microsoft Windows SMB Service Enumeration via \srvsvc
Medium (5.0)	18602	Microsoft Windows SMB svcctl MSRPC Interface SCM Service Enumeration
Medium (5.0)	19998	MS05-045: Vulnerability in Network Connection Manager Could Allow Denial of Service (905414)
Medium (5.0)	21693	MS06-031: Vulnerability in RPC Mutual Authentication Could Allow Spoofing (917736)
Medium (5.0)	42112	MS09-056: Vulnerabilities in Windows CryptoAPI Could Allow Spoofing (974571)
Medium (4.6)	19405	MS05-042: Vulnerability in Kerberos Could Allow Denial of Service, Information Disclosure and Spoofing (899587)
Medium (4.3)	11583	Microsoft Windows shlwapi.dll Malformed HTML Tag Handling Null Pointer DoS
Medium (4.3)	18485	MS05-032: Vulnerability in Microsoft Agent Could Allow Spoofing (890046)
Low (3.3)	16299	MS03-034: NetBIOS Name Service Reply Information Leakage (824105) (credentialed check)
Low (2.6)	10456	Microsoft Windows SMB Service Enumeration
Low (2.6)	11457	Microsoft Windows SMB Registry : Winlogon Cached Password Weakness
Low (2.6)	22333	MS06-053: Vulnerability in Indexing Service Could Allow Cross-Site Scripting (920685)
Info	10395	Microsoft Windows SMB Shares Enumeration
Info	10397	Microsoft Windows SMB LanMan Pipe Server Listing Disclosure
Info	10400	Microsoft Windows SMB Registry Remotely Accessible
Info	10531	Microsoft Windows SMB Registry : Windows 2000 Service Pack Detection
Info	10736	DCE Services Enumeration
Info	10859	Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration
Info	10860	SMB Use Host SID to Enumerate Local Users
Info	10902	Microsoft Windows 'Administrators' Group User List
Info	10904	Microsoft Windows 'Backup Operators' Group User List
Info	10913	Microsoft Windows - Local Users Information : Disabled accounts
Info	10915	Microsoft Windows - Local Users Information : User has never logged on
Info	10916	Microsoft Windows - Local Users Information : Passwords never expire
Info	17651	Microsoft Windows SMB : Obtains the Password Policy
Info	20811	Microsoft Windows Installed Software Enumeration (credentialed check)

Info	23974	Microsoft Windows SMB Share Hosting Office Files
Info	24269	Windows Management Instrumentation (WMI) Available
Info	24270	Computer Manufacturer Information (WMI)
Info	24272	Network Interfaces Enumeration (WMI)
Info	34096	BIOS Version (WMI)
Info	34220	Netstat Portscanner (WMI)
Info	38153	Microsoft Windows Summary of Missing Patches
Info	38689	Microsoft Windows SMB Last Logged On User Disclosure
Info	44401	Microsoft Windows SMB Service Config Enumeration
Info	45590	Common Platform Enumeration (CPE)
Info	48337	Windows ComputerSystemProduct Enumeration (WMI)
Info	48942	Microsoft Windows SMB Registry : OS Version and Processor Architecture
Info	55472	Device Hostname
Info	56468	Time of Last System Startup
Info	57033	Microsoft Patch Bulletin Feasibility Check