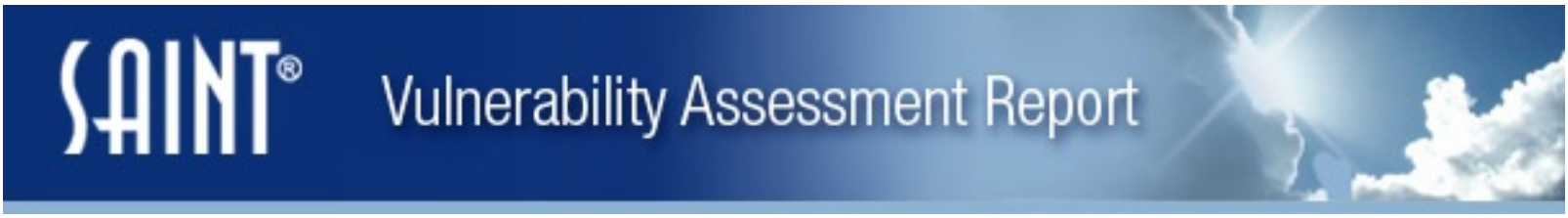


NERC CIP Vulnerability Assessment Report

Report Generated: November 14, 2011

1.0 Background

NERC introduced its Critical Infrastructure Protection (CIP) Reliability Standards CIP-002-1 through CIP-009-1 in 2006. In 2009, it approved version 2 of these standards and began auditing Registered Entities for compliance. All Registered Entities must comply with these eight categories of controls for securing critical cyber assets used to protect the bulk electric system. They include: Cyber Asset Identification, Security Management Controls, Personnel & Training, Electronic Security Perimeter(s), Physical Security, Systems Security Management, Incident Reporting and Response, and Recovery Plans for Critical Cyber Assets. Verification of compliance with CIP shows that a Registered Entity is providing optimal protection for the bulk electric system.

2.0 About this Report

On November 1, 2011, at 11:44 AM, a NERC CIP vulnerability assessment was conducted on the following hosts. The results in the Summary section below document the findings from this scan, to include details about the host, vulnerabilities found, and Common Vulnerability Scoring System (CVSS) numerical score. This scan discovered a total of one live host and detected six critical problems, 139 areas of concern and 28 potential problems. The execution of this vulnerability scan and report directly fulfills CIP requirements for scanning for vulnerabilities in critical cyber assets for the following controls:

CIP-002 Critical Cyber Asset Identification
Identify and document a risk-based assessment method that will be used to identify critical assets. R2 requires an identifiable list and annual asset list review to update all critical cyber assets. Management will approve the list of critical cyber assets. A third-party, without vested interest, shall monitor the compliance to CIP002 outcome of NERC.

CIP-005 Cyber Electronic Security Perimeter(s)
Requires the identification and protection of the Electronic Security Perimeter(s) and Access Points where Cyber Assets reside (R1 and R4).

CIP-007 Cyber Systems Security Management
Define methods, processes and procedures for securing those systems determined to be Critical Cyber Assets (R1 and R3).Document technical and procedural controls to enforce authentication, accountability and user activity (R5). Finally, a third party annual review is required of the perimeter (R8).

The Summary and Details sections provide comprehensive information related to the vulnerabilities - to include content to assess risk and determine remediation.

3.0 Summary

The following vulnerability severity levels are used to categorize the vulnerabilities:

CRITICAL PROBLEMS
Vulnerabilities which pose an immediate threat to the network by allowing a remote attacker to directly gain read or write access, execute commands on the target, or create a denial of service.

AREAS OF CONCERN
Vulnerabilities which do not directly allow remote access, but do allow privilege elevation attacks, attacks on other targets using the vulnerable host as an intermediary, or gathering of passwords or configuration information which could be used to plan an attack.

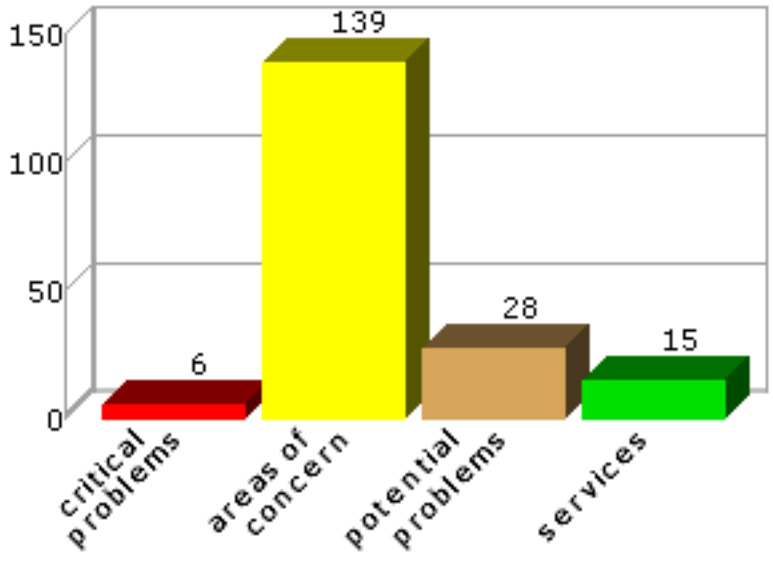
POTENTIAL PROBLEMS
Warnings which may or may not be vulnerabilities, depending upon the patch level or configuration of the target. Further investigation on the part of the system administrator may be necessary.

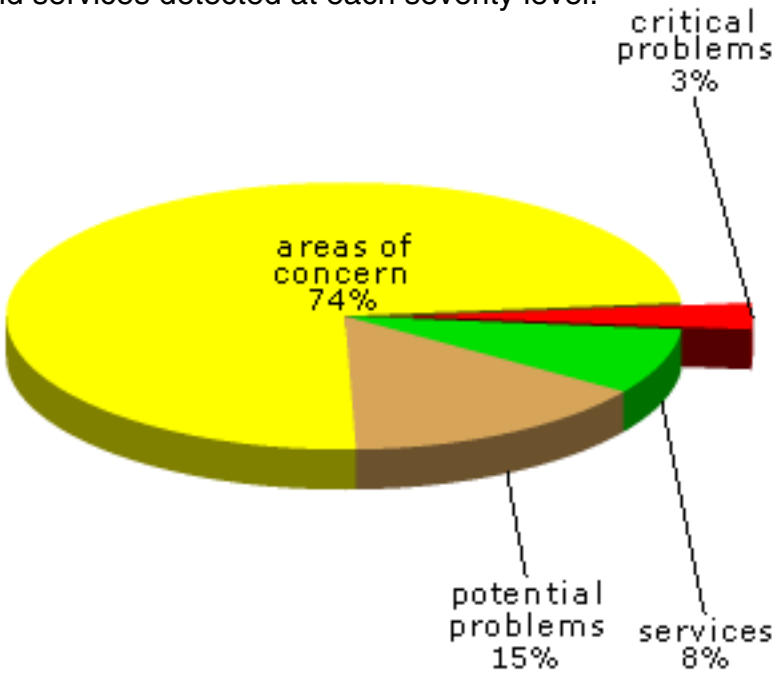
SERVICES
Network services which accept client connections on a given TCP or UDP port. This is simply a count of network services, and does not imply that the service is or is not vulnerable.

The sections below summarize the results of the scan.

3.1 Vulnerabilities by Severity

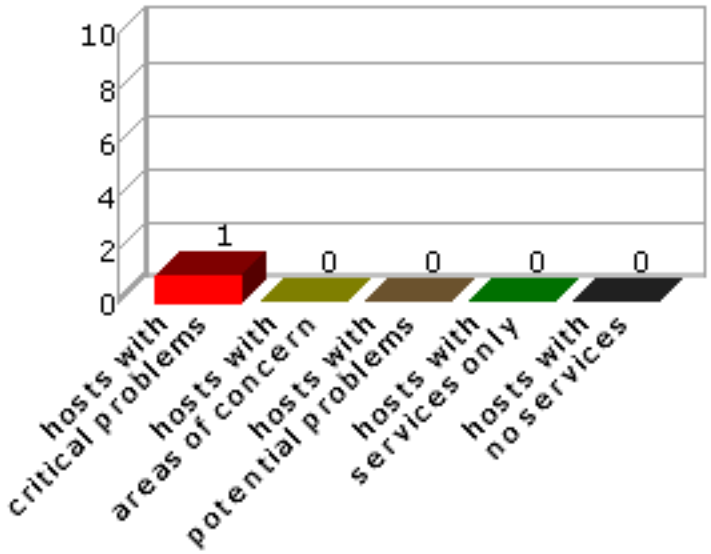
This section shows the overall number of vulnerabilities and services detected at each severity level.





3.2 Hosts by Severity

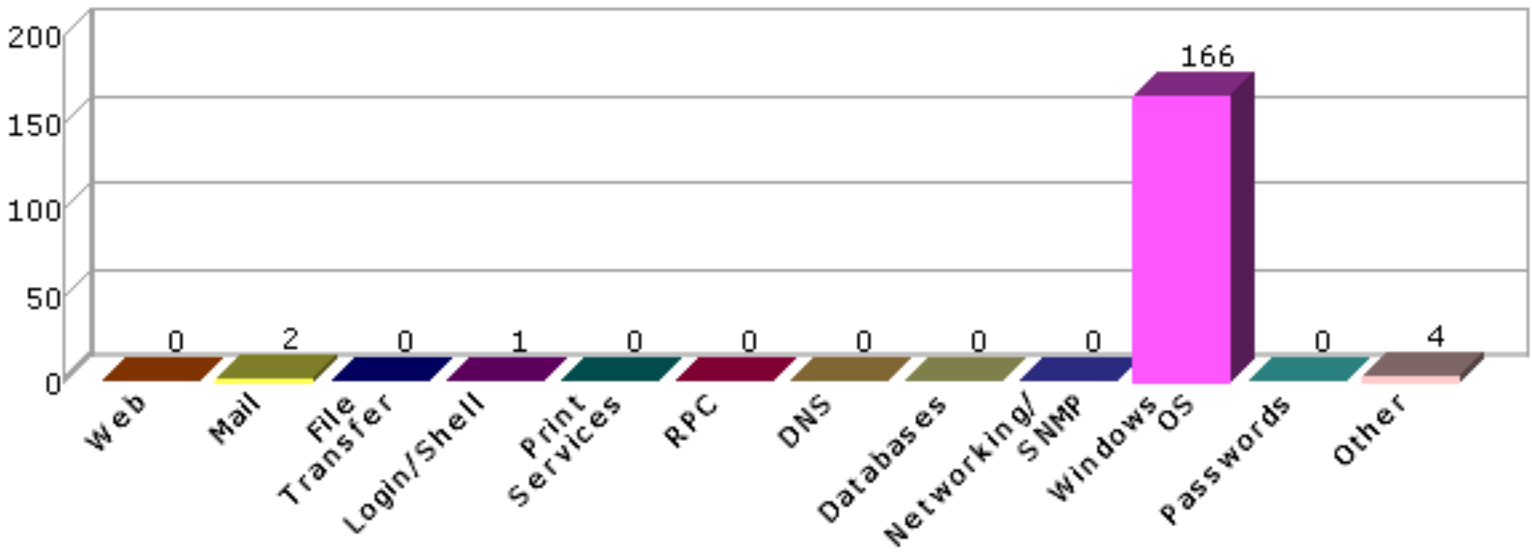
This section shows the overall number of hosts detected at each severity level. The severity level of a host is defined as the highest vulnerability severity level detected on that host.

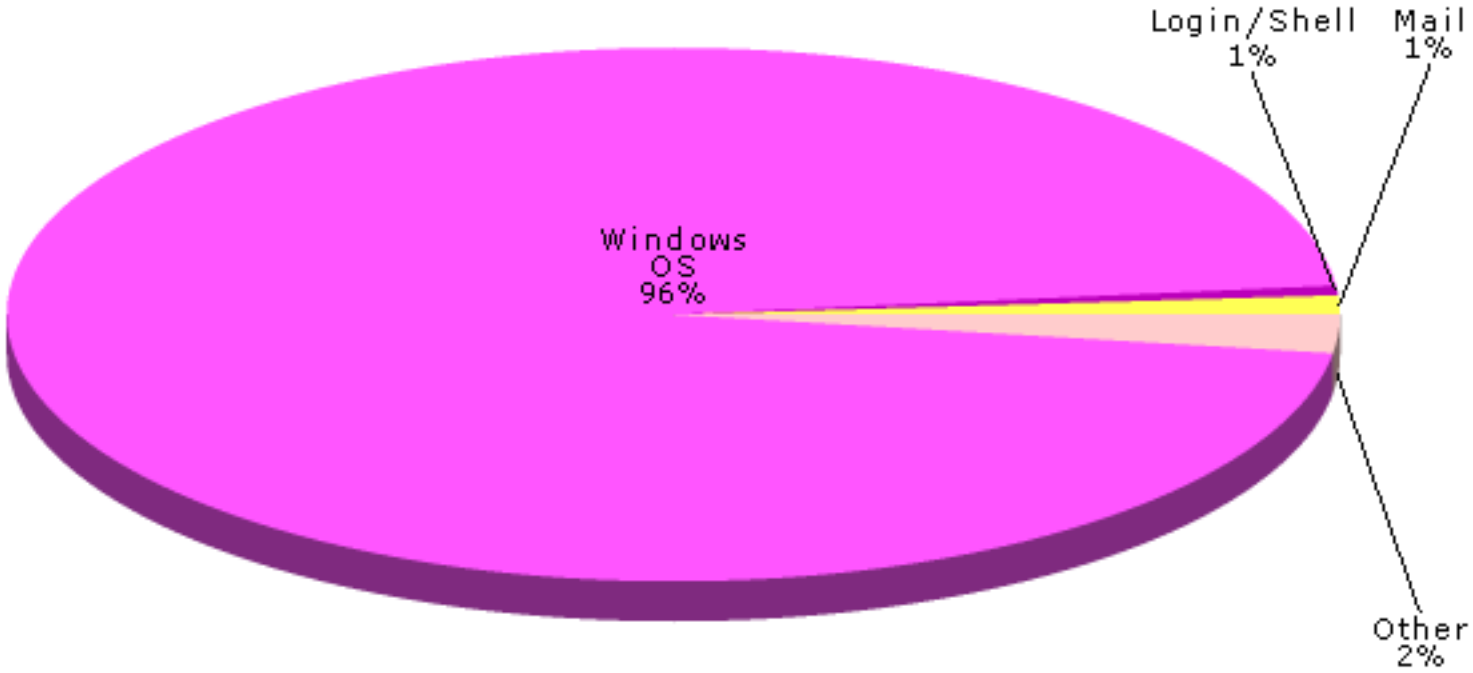


3.3 Vulnerabilities by Class

This section shows the number of vulnerabilities detected in each of the following classes.

Class	Description
Web	Vulnerabilities in web servers, CGI programs, and any other software offering an HTTP interface
Mail	Vulnerabilities in SMTP, IMAP, POP, or web-based mail services
File Transfer	Vulnerabilities in FTP and TFTP services
Login/Shell	Vulnerabilities in ssh, telnet, rlogin, rsh, or rexec services
Print Services	Vulnerabilities in lpd and other print daemons
RPC	Vulnerabilities in Remote Procedure Call services
DNS	Vulnerabilities in Domain Name Services
Databases	Vulnerabilities in database services
Networking/SNMP	Vulnerabilities in routers, switches, firewalls, or any SNMP service
Windows OS	Missing hotfixes or vulnerabilities in the registry or SMB shares
Passwords	Missing or easily guessed user passwords
Other	Any vulnerability which does not fit into one of the above classes





4.0 Overview

The following tables present an overview of the hosts discovered on the network and the vulnerabilities contained therein.

4.1 Host List

This table presents an overview of the hosts discovered on the network.

Host Name	Netbios Name	IP Address	Host Type	Critical Problems	Areas of Concern	Potential Problems
win2003unpatch.sainttest.local	WIN2003UNPATCH	10.7.0.11	Windows Server 2003 SP2	6	139	28

4.2 Vulnerability List

This table presents an overview of the vulnerabilities detected on the network.

Host Name	Severity	Vulnerability / Service	Class	CVE	Exploit Available?
win2003unpatch.sainttest.local	critical	Microsoft Remote Desktop Protocol Denial of Service Vulnerability (MS11-065)	Windows OS	CVE-2011-1968	no
win2003unpatch.sainttest.local	critical	Microsoft Windows TCP/IP remote code execution vulnerability (MS09-048)	Windows OS	CVE-2006-2379 CVE-2008-4609 CVE-2009-1926	no
win2003unpatch.sainttest.local	critical	Windows RPC authentication denial of service	Windows OS	CVE-2007-2228	no
win2003unpatch.sainttest.local	critical	Windows SMB Server Transaction Vulnerability	Windows OS	CVE-2011-0661	no
win2003unpatch.sainttest.local	critical	Windows Server Service MS08-067 buffer overflow	Windows OS	CVE-2008-4250	yes
win2003unpatch.sainttest.local	critical	vulnerable version of SMB Server (MS10-012) dated 2007-2-17	Windows OS	CVE-2010-0020 CVE-2010-0021 CVE-2010-0022 CVE-2010-0231	no

win2003unpatch.sainttest.local	concern	Internet Explorer 6 vulnerable version, mshtml.dll dated 2007-2-17	Windows OS	CVE-2007-0218 CVE-2007-0942 CVE-2007-0944 CVE-2007-0945 CVE-2007-1091 CVE-2007-1750 CVE-2007-1751 CVE-2007-2216 CVE-2007-2221 CVE-2007-2222 CVE-2007-3027 CVE-2007-3041 CVE-2007-3091 CVE-2007-3826 CVE-2007-3892 CVE-2007-3893 CVE-2007-3902 CVE-2007-3903 CVE-2007-4790 CVE-2007-5158 CVE-2007-5344 CVE-2007-5347 CVE-2008-0076 CVE-2008-0077 CVE-2008-0078 CVE-2008-1085 CVE-2008-1442 CVE-2008-1544 CVE-2008-2254 CVE-2008-2255 CVE-2008-2256 CVE-2008-2257 CVE-2008-2258 CVE-2008-2259 CVE-2008-2947 CVE-2008-3472 CVE-2008-3473 CVE-2008-3474 CVE-2008-3475 CVE-2008-3476 CVE-2008-4261 CVE-2008-4844 CVE-2009-0550 CVE-2009-0551 CVE-2009-0552 CVE-2009-0553 CVE-2009-0554 CVE-2009-1140 CVE-2009-1141 CVE-2009-1528 CVE-2009-1547 CVE-2009-1917 CVE-2009-1918 CVE-2009-1919 CVE-2009-2493 CVE-2009-2529 CVE-2009-2530 CVE-2009-2531 CVE-2009-3672 CVE-2010-0244 CVE-2010-0247 CVE-2010-0248 CVE-2010-0249

				CVE-2010-0255 CVE-2010-0267 CVE-2010-0488 CVE-2010-0489 CVE-2010-0490 CVE-2010-0491 CVE-2010-0494 CVE-2010-0805 CVE-2010-0806 CVE-2010-0808 CVE-2010-1258 CVE-2010-1259 CVE-2010-1262 CVE-2010-2556 CVE-2010-2557 CVE-2010-2558 CVE-2010-2560 CVE-2010-3325 CVE-2010-3326 CVE-2010-3327 CVE-2010-3328 CVE-2010-3330 CVE-2010-3331 CVE-2010-3340 CVE-2010-3342 CVE-2010-3343 CVE-2010-3346 CVE-2010-3348 CVE-2010-3962 CVE-2010-3971 CVE-2011-0035 CVE-2011-0036 CVE-2011-0094 CVE-2011-0346 CVE-2011-1244 CVE-2011-1245 CVE-2011-1250 CVE-2011-1254 CVE-2011-1255 CVE-2011-1256 CVE-2011-1257 CVE-2011-1258 CVE-2011-1261 CVE-2011-1345 CVE-2011-1960 CVE-2011-1961 CVE-2011-1962 CVE-2011-1964 CVE-2011-1993 CVE-2011-1995 CVE-2011-1996 CVE-2011-1997 CVE-2011-2000 CVE-2011-2001 CVE-2011-2383	yes
win2003unpatch.sainttest.local	concern	Internet Explorer VBScript and JScript decoding vulnerability	Windows OS	CVE-2008-0083	no
win2003unpatch.sainttest.local	concern	Internet Explorer VBScript and JScript memory reallocation vulnerability (MS11-031)	Windows OS	CVE-2011-0663	no

win2003unpatch.sainttest.local	concern	Internet Explorer vulnerable VML version dated 2007-2-17	Windows OS	CVE-2007-1749 CVE-2011-1266	no
win2003unpatch.sainttest.local	concern	Jscript.dll buffer overflow vulnerability	Windows OS	CVE-2009-1920	no
win2003unpatch.sainttest.local	concern	sapi.dll ActiveX vulnerability	Windows OS	CVE-2007-0675	no
win2003unpatch.sainttest.local	concern	Macrovision SafeDisc driver local privilege elevation	Windows OS	CVE-2007-5587	no
win2003unpatch.sainttest.local	concern	Information disclosure vulnerability in .NET Framework	Windows OS	CVE-2011-1978	no
win2003unpatch.sainttest.local	concern	MS11-028 Vulnerability in .NET Framework Could Allow Remote Code Execution	Windows OS	CVE-2010-3958	no
win2003unpatch.sainttest.local	concern	MS11-039 Vulnerability in .NET Framework Could Allow Remote Code Execution	Windows OS	CVE-2011-0664	no
win2003unpatch.sainttest.local	concern	MS11-044 Vulnerability in .NET Framework Could Allow Remote Code Execution	Windows OS	CVE-2011-1271	no
win2003unpatch.sainttest.local	concern	MS11-078 Vulnerability in .NET Framework Could Allow Remote Code Execution	Windows OS	CVE-2011-1253	no
win2003unpatch.sainttest.local	concern	Microsoft .NET CLR virtual method delegate vulnerability	Windows OS	CVE-2010-1898	no
win2003unpatch.sainttest.local	concern	Microsoft .NET Common Language Runtime Could Allow Remote Code Execution	Windows OS	CVE-2009-0090 CVE-2009-0091 CVE-2009-2497	no
win2003unpatch.sainttest.local	concern	Microsoft .NET Framework Could Allow Tampering	Windows OS	CVE-2009-0217	no
win2003unpatch.sainttest.local	concern	Microsoft outlook ATL vulnerability (MS09-037)	Windows OS	CVE-2008-0015 CVE-2008-0020 CVE-2009-0901 CVE-2009-2493 CVE-2009-2494	yes
win2003unpatch.sainttest.local	concern	Outlook Express Could Allow Remote Code Execution (MS10-030)	Windows OS	CVE-2010-0816	no
win2003unpatch.sainttest.local	concern	Windows MHTML protocol handler vulnerability	Windows OS	CVE-2008-1448	no
win2003unpatch.sainttest.local	concern	fraudulent Comodo certificates not in disallowed store	Windows OS		no
win2003unpatch.sainttest.local	concern	fraudulent DigiNotar certificates not in disallowed store	Windows OS		no
win2003unpatch.sainttest.local	concern	Telnet Authentication Reflection	Login /Shell	CVE-2009-1930	yes
win2003unpatch.sainttest.local	concern	Insecure Library Loading in Outlook Express WAB.EXE Could Allow Remote Code Execution	Mail	CVE-2010-3147	no
win2003unpatch.sainttest.local	concern	Outlook Express vulnerable version, inetcomm.dll dated 2007-2-17	Mail	CVE-2006-2111 CVE-2007-2225 CVE-2007-2227 CVE-2007-3897	no
win2003unpatch.sainttest.local	concern	Elevation of Privilege Vulnerabilities in Windows Kerberos (MS11-013)	Other	CVE-2011-0043	no
win2003unpatch.sainttest.local	concern	Ancillary Function Driver Vulnerability (MS11-046)	Windows OS	CVE-2011-1249	no
win2003unpatch.sainttest.local	concern	Ancillary Function Driver Vulnerability (MS11-080)	Windows OS	CVE-2011-2005	no

win2003unpatch.sainttest.local	concern	Blended threat privilege elevation vulnerability	Windows OS	CVE-2008-2540	no
win2003unpatch.sainttest.local	concern	DirectX MJPEG decompression remote code execution vulnerability	Windows OS	CVE-2009-0084	no
win2003unpatch.sainttest.local	concern	DirectX SAMI-MJPEG parsing remote code execution for DirectX 9.0c	Windows OS	CVE-2008-0011	no
win2003unpatch.sainttest.local	concern	DirectX parsing remote code execution for DirectX 9.0c	Windows OS	CVE-2007-3895	no
win2003unpatch.sainttest.local	concern	Elevation of Privilege Vulnerabilities in Windows (MS09-012)	Windows OS	CVE-2008-1436 CVE-2009-0078 CVE-2009-0079	no
win2003unpatch.sainttest.local	concern	Elevation of Privilege Vulnerabilities in Windows (MS10-015)	Windows OS	CVE-2010-0232 CVE-2010-0233	no
win2003unpatch.sainttest.local	concern	Elevation of Privilege Vulnerabilities in Windows (MS11-062)	Windows OS	CVE-2011-1974	no
win2003unpatch.sainttest.local	concern	Insecure Library Loading in Internet Connection Signup Wizard Could Allow Remote Code Execution	Windows OS	CVE-2010-3144	no
win2003unpatch.sainttest.local	concern	Kernel-Mode Drivers vulnerabilities	Windows OS	CVE-2011-0086 CVE-2011-0087 CVE-2011-0088 CVE-2011-0089 CVE-2011-0090	no
win2003unpatch.sainttest.local	concern	MHTML Mime-formatted information disclosure	Windows OS	CVE-2011-1894	no
win2003unpatch.sainttest.local	concern	MPEG 4 codec remote code execution vulnerability (MS10-062)	Windows OS	CVE-2010-0818	no
win2003unpatch.sainttest.local	concern	MS11-034 Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege	Windows OS	CVE-2011-0662 CVE-2011-0665 CVE-2011-0666 CVE-2011-0667 CVE-2011-0670 CVE-2011-0671 CVE-2011-0672 CVE-2011-0674 CVE-2011-0675 CVE-2011-0676 CVE-2011-0677 CVE-2011-1225 CVE-2011-1226 CVE-2011-1227 CVE-2011-1228 CVE-2011-1229 CVE-2011-1230 CVE-2011-1231 CVE-2011-1232 CVE-2011-1233 CVE-2011-1234 CVE-2011-1235 CVE-2011-1236 CVE-2011-1237 CVE-2011-1238 CVE-2011-1239 CVE-2011-1240 CVE-2011-1241 CVE-2011-1242	no
win2003unpatch.sainttest.local	concern	MS11-077 Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution	Windows OS	CVE-2011-1985 CVE-2011-2003 CVE-2011-2011	no

win2003unpatch.sainttest.local	concern	Microsoft AFD Kernel Overwrite vulnerability	Windows OS	CVE-2008-3464	no
win2003unpatch.sainttest.local	concern	Microsoft Active Accessibility Insecure Library Loading Vulnerability (MS11-075)	Windows OS	CVE-2011-1247	no
win2003unpatch.sainttest.local	concern	Microsoft Agent URL parsing vulnerability	Windows OS	CVE-2007-1205	no
win2003unpatch.sainttest.local	concern	Microsoft Data Access Component remote code execution (MS11-002)	Windows OS	CVE-2011-0026 CVE-2011-0027	no
win2003unpatch.sainttest.local	concern	Microsoft DirectShow Quartz AVI buffer overflow	Windows OS	CVE-2010-0250	no
win2003unpatch.sainttest.local	concern	Microsoft DirectShow QuickTime Movie Parsing Code Execution	Windows OS	CVE-2009-1537 CVE-2009-1538 CVE-2009-1539	yes
win2003unpatch.sainttest.local	concern	Microsoft Graphics Rendering Engine Thumbnail Image Stack Buffer Overflow	Windows OS	CVE-2010-3970	yes
win2003unpatch.sainttest.local	concern	Microsoft Image Color Management System vulnerable version, mscms.dll dated 2007-2-17	Windows OS	CVE-2008-2245	no
win2003unpatch.sainttest.local	concern	Microsoft Paint Integer Overflow vulnerability	Windows OS	CVE-2010-0028	no
win2003unpatch.sainttest.local	concern	Microsoft Video ActiveX Control Stack Buffer Overflow	Windows OS	CVE-2008-0015	yes
win2003unpatch.sainttest.local	concern	Microsoft Windows DHTML remote code execution vulnerability (MS09-046)	Windows OS	CVE-2009-2519	no
win2003unpatch.sainttest.local	concern	Microsoft Windows OpenType CFF vulnerability (MS11-032)	Windows OS	CVE-2011-0034	no
win2003unpatch.sainttest.local	concern	Microsoft Windows OpenType Compact Font Format driver Remote Code Execution Vulnerability	Windows OS	CVE-2011-0033	no
win2003unpatch.sainttest.local	concern	Microsoft Windows Shell remote code execution vulnerability	Windows OS	CVE-2010-2568	yes
win2003unpatch.sainttest.local	concern	Microsoft Windows vulnerable version, msconv97.dll dated 2006-3-22	Windows OS	CVE-2009-2506	no
win2003unpatch.sainttest.local	concern	Microsoft XML Core Services vulnerable version dated 2007-2-17	Windows OS	CVE-2007-0099 CVE-2007-2223 CVE-2008-4029 CVE-2008-4033 CVE-2010-2561	no
win2003unpatch.sainttest.local	concern	Multiple GDI vulnerabilities fixed by MS07-017	Windows OS	CVE-2006-5586 CVE-2006-5758 CVE-2007-0038 CVE-2007-1211 CVE-2007-1212 CVE-2007-1213 CVE-2007-1215	yes
win2003unpatch.sainttest.local	concern	OpenType Font format driver remote code execution	Windows OS	CVE-2010-3956 CVE-2010-3957 CVE-2010-3959	no
win2003unpatch.sainttest.local	concern	Over-the-network SMB packet vulnerabilities in Windows system (MS10-054)	Windows OS	CVE-2010-2550 CVE-2010-2551 CVE-2010-2552	no
win2003unpatch.sainttest.local	concern	Shell32.dll Windows URI handling Remote Code Execution	Windows OS	CVE-2007-3896	yes
win2003unpatch.sainttest.local	concern	Uniscribe Font Parsing Engine Memory Corruption (MS10-063)	Windows OS	CVE-2010-2738	no

win2003unpatch.sainttest.local	concern	Vulnerabilities in SChannel could allow Remote Code Execution	Windows OS	CVE-2009-3555 CVE-2010-2566	no
win2003unpatch.sainttest.local	concern	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (MS11-054)	Windows OS	CVE-2011-1874 CVE-2011-1875 CVE-2011-1876 CVE-2011-1877 CVE-2011-1878 CVE-2011-1879 CVE-2011-1880 CVE-2011-1881 CVE-2011-1882 CVE-2011-1883 CVE-2011-1884 CVE-2011-1885 CVE-2011-1886 CVE-2011-1887 CVE-2011-1888	no
win2003unpatch.sainttest.local	concern	Vulnerability in the OpenType Compact Font Format Driver Could Allow Elevation of Privilege	Windows OS	CVE-2010-0819 CVE-2010-2740 CVE-2010-2741	no
win2003unpatch.sainttest.local	concern	Win32 API parameter validation vulnerability	Windows OS	CVE-2007-2219	no
win2003unpatch.sainttest.local	concern	Windows 2003 GDI vulnerable version, gdi32.dll dated 2007-2-17	Windows OS	CVE-2008-1083 CVE-2008-1087 CVE-2008-2249 CVE-2008-3465	yes
win2003unpatch.sainttest.local	concern	Windows ASN1 spoofing vulnerability	Windows OS	CVE-2009-2510 CVE-2009-2511	no
win2003unpatch.sainttest.local	concern	Windows Authenticode Signature Verification (MS10-019) version, wintrust.dll dated 2007-2-17	Windows OS	CVE-2010-0486	no
win2003unpatch.sainttest.local	concern	Windows CSRSS (MS11-010) vulnerable version, csrsrv.dll dated 2007-2-17	Windows OS	CVE-2011-0030	no
win2003unpatch.sainttest.local	concern	Windows CSRSS (MS11-056) vulnerable version, winsrv.dll dated 2007-2-17	Windows OS	CVE-2011-1281 CVE-2011-1282 CVE-2011-1283 CVE-2011-1284 CVE-2011-1870	no
win2003unpatch.sainttest.local	concern	Windows CSRSS (MS11-063) vulnerable version, winsrv.dll dated 2007-2-17	Windows OS	CVE-2011-1967	no
win2003unpatch.sainttest.local	concern	Windows CSRSS Local (MS10-011) vulnerable version, csrsrv.dll dated 2007-2-17	Windows OS	CVE-2010-0023	no
win2003unpatch.sainttest.local	concern	Windows CSRSS remote code execution	Windows OS	CVE-2006-6696 CVE-2006-6797	no
win2003unpatch.sainttest.local	concern	Windows Cabinet File Viewer (MS10-019) version, cabview.dll dated 2007-2-17	Windows OS	CVE-2010-0487	no
win2003unpatch.sainttest.local	concern	Windows Client Server Runtime Subsystem Could Allow Elevation of Privilege	Windows OS	CVE-2010-1891	no
win2003unpatch.sainttest.local	concern	Windows DNS Client Spoofing vulnerability (MS08-037)	Windows OS	CVE-2008-1447	no
win2003unpatch.sainttest.local	concern	Windows DNS Resolution Vulnerability	Windows OS	CVE-2011-0657	no
win2003unpatch.sainttest.local	concern	Windows DNS Spoofing vulnerability	Windows OS	CVE-2008-0087	no

win2003unpatch.sainttest.local	concern	Windows DirectShow AVI Filter buffer overflow	Windows OS	CVE-2010-0250	no
win2003unpatch.sainttest.local	concern	Windows Embedded OpenType Font Engine vulnerabilities	Windows OS	CVE-2009-0231 CVE-2009-0232	no
win2003unpatch.sainttest.local	concern	Windows Fax Cover Page Remote Code Execution Vulnerability (MS11-024)	Windows OS	CVE-2010-3974 CVE-2010-4701	yes
win2003unpatch.sainttest.local	concern	Windows Help and Support Center trusted document whitelist bypass (MS10-042)	Windows OS	CVE-2010-1885	yes
win2003unpatch.sainttest.local	concern	Windows IME vulnerable to library injection (MS11-071)	Windows OS	CVE-2011-1991	no
win2003unpatch.sainttest.local	concern	Windows ISATAP Component spoofing vulnerability (MS10-029)	Windows OS	CVE-2010-0812	no
win2003unpatch.sainttest.local	concern	Windows Internet Authentication Service vulnerabilities	Windows OS	CVE-2009-3677	no
win2003unpatch.sainttest.local	concern	Windows Kernel privilege elevation (ms07-022) vulnerability	Windows OS	CVE-2007-1206	no
win2003unpatch.sainttest.local	concern	Windows LPC Elevation of Privilege vulnerability (MS10-084)	Windows OS	CVE-2010-3222	no
win2003unpatch.sainttest.local	concern	Windows LSASS IPSEC Denial-of-Service Vulnerability	Windows OS	CVE-2009-3675	no
win2003unpatch.sainttest.local	concern	Windows LSASS length validation vulnerability	Windows OS	CVE-2011-0039	no
win2003unpatch.sainttest.local	concern	Windows LSASS vulnerability	Windows OS	CVE-2007-5352	no
win2003unpatch.sainttest.local	concern	Windows MHTML script injection vulnerability (MS11-026)	Windows OS	CVE-2011-0096	no
win2003unpatch.sainttest.local	concern	Windows MPEG Layer-3 Audio Decoder vulnerable version, l3codecx.ax dated 2006-3-22	Windows OS	CVE-2010-1882	no
win2003unpatch.sainttest.local	concern	Windows MPEG layer 3 codec vulnerable version, l3codecx.ax dated 2006-3-22	Windows OS	CVE-2010-0480	no
win2003unpatch.sainttest.local	concern	Windows Media Format ASF file parsing vulnerability	Windows OS	CVE-2007-0064	no
win2003unpatch.sainttest.local	concern	Windows Media Player ASX Playlist Parsing Buffer Overflow	Windows OS	CVE-2006-4702 CVE-2006-6134	no
win2003unpatch.sainttest.local	concern	Windows Media Player Memory Corruption Vulnerability (MS10-082)	Windows OS	CVE-2010-2745	no
win2003unpatch.sainttest.local	concern	Windows Media Player Skin parsing and decompression remote code execution	Windows OS	CVE-2007-3035 CVE-2007-3037	no
win2003unpatch.sainttest.local	concern	Windows Media decompression vulnerabilities	Windows OS	CVE-2010-1879 CVE-2010-1880	no
win2003unpatch.sainttest.local	concern	Windows OLE Automation Underflow vulnerability (MS11-038)	Windows OS	CVE-2011-0658	no
win2003unpatch.sainttest.local	concern	Windows OLE Automation remote code execution vulnerability	Windows OS	CVE-2007-0065 CVE-2007-2224	no
win2003unpatch.sainttest.local	concern	Windows RPC Marshalling Engine vulnerability	Windows OS	CVE-2009-0568	no
win2003unpatch.sainttest.local	concern	Windows RPC Memory Corruption vulnerability	Windows OS	CVE-2010-2567	no
win2003unpatch.sainttest.local	concern	Windows Remote Desktop Connection vulnerabilities	Windows OS	CVE-2009-1133 CVE-2009-1929	no
win2003unpatch.sainttest.local	concern	Windows SMB Client vulnerabilities (MS10-006)	Windows OS	CVE-2010-0016	no

win2003unpatch.sainttest.local	concern	Windows SMB Client vulnerabilities (MS10-020)	Windows OS	CVE-2009-3676 CVE-2010-0269 CVE-2010-0270 CVE-2010-0476 CVE-2010-0477	no
win2003unpatch.sainttest.local	concern	Windows SMB Client vulnerabilities (MS11-019)	Windows OS	CVE-2011-0654 CVE-2011-0660	no
win2003unpatch.sainttest.local	concern	Windows SMB Client vulnerabilities (MS11-043)	Windows OS	CVE-2011-1268	no
win2003unpatch.sainttest.local	concern	Windows SMB Remote Code Execution	Windows OS	CVE-2008-4038	no
win2003unpatch.sainttest.local	concern	Windows SMB credential reflection vulnerability	Windows OS	CVE-2008-4037	yes
win2003unpatch.sainttest.local	concern	Windows Schannel digital signature parsing vulnerability	Windows OS	CVE-2007-2218	no
win2003unpatch.sainttest.local	concern	Windows Schannel spoofing vulnerability	Windows OS	CVE-2009-0085	no
win2003unpatch.sainttest.local	concern	Windows Shell Handler vulnerability	Windows OS	CVE-2010-0027	no
win2003unpatch.sainttest.local	concern	Windows VB script vulnerable version, vbscript.dll dated 2007-2-17	Windows OS	CVE-2010-0483 CVE-2011-0031	no
win2003unpatch.sainttest.local	concern	Windows Virtual Address Descriptor integer overflow	Windows OS	CVE-2008-4036	no
win2003unpatch.sainttest.local	concern	Windows WMA Voice codec vulnerability	Windows OS	CVE-2009-0555 CVE-2009-2525	no
win2003unpatch.sainttest.local	concern	Windows WordPad Converter (MS11-033) vulnerable version, mswrd8.wpc dated 2007-2-17	Windows OS	CVE-2011-0028	no
win2003unpatch.sainttest.local	concern	Windows atl.dll vulnerable (MS09-037)	Windows OS	CVE-2008-0015 CVE-2008-0020 CVE-2009-0901 CVE-2009-2493 CVE-2009-2494	yes
win2003unpatch.sainttest.local	concern	Windows dhtmled.ocx vulnerable (MS09-037)	Windows OS	CVE-2008-0015 CVE-2008-0020 CVE-2009-0901 CVE-2009-2493 CVE-2009-2494	yes
win2003unpatch.sainttest.local	concern	Windows event system subscription request and pointer array vulnerabilities	Windows OS	CVE-2008-1456 CVE-2008-1457	no
win2003unpatch.sainttest.local	concern	Windows kernel GDI validation vulnerabilities	Windows OS	CVE-2009-0081 CVE-2009-0082 CVE-2009-0083	no
win2003unpatch.sainttest.local	concern	Windows kernel NDProxy privilege elevation vulnerability (MS10-099)	Windows OS	CVE-2010-3963	no
win2003unpatch.sainttest.local	concern	Windows kernel desktop validation vulnerabilities	Windows OS	CVE-2009-1123 CVE-2009-1124 CVE-2009-1125 CVE-2009-1126	no
win2003unpatch.sainttest.local	concern	Windows kernel embedded font vulnerabilities	Windows OS	CVE-2009-1127 CVE-2009-2513 CVE-2009-2514	no
win2003unpatch.sainttest.local	concern	Windows kernel multiple privilege elevation vulnerabilities (MS10-048)	Windows OS	CVE-2010-1887 CVE-2010-1894 CVE-2010-1895 CVE-2010-1896 CVE-2010-1897	no
win2003unpatch.sainttest.local	concern	Windows kernel multiple privilege elevation vulnerabilities (MS10-073)	Windows OS	CVE-2010-2743 CVE-2010-2744	no

win2003unpatch.sainttest.local	concern	Windows kernel multiple privilege elevation vulnerabilities (MS10-098)	Windows OS	CVE-2010-3939 CVE-2010-3940 CVE-2010-3941 CVE-2010-3942 CVE-2010-3943	no
win2003unpatch.sainttest.local	concern	Windows kernel property validation vulnerabilities	Windows OS	CVE-2008-2250 CVE-2008-2251 CVE-2008-2252	no
win2003unpatch.sainttest.local	concern	Windows kernel user mode callback vulnerability	Windows OS	CVE-2008-1084	no
win2003unpatch.sainttest.local	concern	Windows kernel vulnerable (MS10-021) version, ntoskrnl.exe dated 2007-2-17	Windows OS	CVE-2010-0234 CVE-2010-0235 CVE-2010-0236 CVE-2010-0237 CVE-2010-0238 CVE-2010-0481 CVE-2010-0482 CVE-2010-0810	no
win2003unpatch.sainttest.local	concern	Windows kernel vulnerable (MS11-011) version, ntoskrnl.exe dated 2007-2-17	Windows OS	CVE-2010-4398	no
win2003unpatch.sainttest.local	concern	Windows kernel vulnerable version, ntoskrnl.exe dated 2007-2-17	Windows OS	CVE-2009-2515 CVE-2009-2516 CVE-2009-2517	no
win2003unpatch.sainttest.local	concern	Windows media file processing vulnerable (MS09-038)	Windows OS	CVE-2009-1545 CVE-2009-1546	no
win2003unpatch.sainttest.local	concern	Windows print spooler vulnerabilities	Windows OS	CVE-2009-0229 CVE-2009-0230	no
win2003unpatch.sainttest.local	concern	Word 97 Converter vulnerable version, mswrd8.wpc dated 2007-2-17	Windows OS	CVE-2008-4841 CVE-2009-0235	yes
win2003unpatch.sainttest.local	concern	WordPad Word 97 Text Converter (MS10-067) version, mswrd8.wpc dated 2007-2-17	Windows OS	CVE-2010-2563	no
win2003unpatch.sainttest.local	concern	Wordpad COM validation (MS10-083) version, ole32.dll dated 2007-2-17	Windows OS	CVE-2010-1263	no
win2003unpatch.sainttest.local	concern	Workstation Service Elevation of Privilege	Windows OS	CVE-2009-1544	no
win2003unpatch.sainttest.local	concern	comctl32.dll remote code execution vulnerability (MS10-081)	Windows OS	CVE-2010-2746	no
win2003unpatch.sainttest.local	concern	mfc40.dll remote code execution vulnerability (MS10-074)	Windows OS	CVE-2010-3227	no
win2003unpatch.sainttest.local	concern	t2embed.dll remote code execution vulnerability (MS10-076)	Windows OS	CVE-2010-1883	no
win2003unpatch.sainttest.local	potential	AV Information: AntiVirus software not found (AVG F-Secure Forefront McAfee Symantec TrendMicro)	Other		no
win2003unpatch.sainttest.local	potential	ICMP timestamp requests enabled	Other	CVE-1999-0524	no
win2003unpatch.sainttest.local	potential	Internet Explorer Shell.Explorer object enabled	Windows OS		no
win2003unpatch.sainttest.local	potential	last user name shown in login box	Windows OS	CVE-1999-0592	no
win2003unpatch.sainttest.local	potential	password complexity policy disabled	Windows OS	CVE-1999-0535	no
win2003unpatch.sainttest.local	potential	weak account lockout policy (0)	Windows OS	CVE-1999-0582	no
win2003unpatch.sainttest.local	potential	weak minimum password age policy (0 days)	Windows OS	CVE-1999-0535	no

win2003unpatch.sainttest.local	potential	weak minimum password length policy (0)	Windows OS	CVE-1999-0535	no
win2003unpatch.sainttest.local	potential	weak password history policy (0)	Windows OS	CVE-1999-0535	no
win2003unpatch.sainttest.local	potential	non-administrative users can bypass traverse checking	Windows OS	CVE-1999-0534	no
win2003unpatch.sainttest.local	potential	non-administrative users can replace a process level token	Windows OS	CVE-1999-0534	no
win2003unpatch.sainttest.local	potential	account management auditing disabled	Windows OS	CVE-1999-0575	no
win2003unpatch.sainttest.local	potential	account management failure auditing disabled	Windows OS	CVE-1999-0575	no
win2003unpatch.sainttest.local	potential	logon failure auditing disabled	Windows OS	CVE-1999-0575	no
win2003unpatch.sainttest.local	potential	object access auditing disabled	Windows OS	CVE-1999-0575	no
win2003unpatch.sainttest.local	potential	object access failure auditing disabled	Windows OS	CVE-1999-0575	no
win2003unpatch.sainttest.local	potential	policy change auditing disabled	Windows OS	CVE-1999-0575	no
win2003unpatch.sainttest.local	potential	policy change failure auditing disabled	Windows OS	CVE-1999-0575	no
win2003unpatch.sainttest.local	potential	system event auditing disabled	Windows OS	CVE-1999-0575	no
win2003unpatch.sainttest.local	potential	system event failure auditing disabled	Windows OS	CVE-1999-0575	no
win2003unpatch.sainttest.local	potential	Windows administrator account not renamed	Windows OS	CVE-1999-0585	no
win2003unpatch.sainttest.local	potential	Windows guest account not renamed	Windows OS		no
win2003unpatch.sainttest.local	potential	Password never expires for user localuser	Windows OS		no
win2003unpatch.sainttest.local	potential	Windows TCP/IP Stack not hardened	Other		no
win2003unpatch.sainttest.local	potential	Microsoft Windows Insecure Library Loading vulnerability	Windows OS		no
win2003unpatch.sainttest.local	potential	Microsoft Windows Service Isolation Bypass Local Privilege Escalation	Windows OS	CVE-2010-1886	no
win2003unpatch.sainttest.local	potential	Multiple Windows TCP/IP vulnerabilities (MS08-001)	Windows OS	CVE-2007-0066 CVE-2007-0069	no
win2003unpatch.sainttest.local	potential	Windows Embedded OpenType Font Engine Vulnerability	Windows OS	CVE-2010-0018	no
win2003unpatch.sainttest.local	service	1025/UDP			no
win2003unpatch.sainttest.local	service	1038/TCP			no
win2003unpatch.sainttest.local	service	1718/UDP			no
win2003unpatch.sainttest.local	service	1719/UDP			no
win2003unpatch.sainttest.local	service	DNS			no
win2003unpatch.sainttest.local	service	SMB			no
win2003unpatch.sainttest.local	service	XDM (X login)			no
win2003unpatch.sainttest.local	service	epmap (135/TCP)			no
win2003unpatch.sainttest.local	service	isakmp (500/UDP)			no
win2003unpatch.sainttest.local	service	microsoft-ds (445/TCP)			no
win2003unpatch.sainttest.local	service	microsoft-ds (445/UDP)			no
win2003unpatch.sainttest.local	service	netbios-dgm (138/UDP)			no
win2003unpatch.sainttest.local	service	netbios-ns (137/UDP)			no
win2003unpatch.sainttest.local	service	ntp (123/UDP)			no
win2003unpatch.sainttest.local	service	tftp (69/UDP)			no

win2003unpatch.sainttest.local	info	User: Administrator (500)	no
win2003unpatch.sainttest.local	info	User: Guest (501) (disabled)	no
win2003unpatch.sainttest.local	info	User: HelpServicesGroup (1000)	no
win2003unpatch.sainttest.local	info	User: SUPPORT_388945a0 (1001) (disabled)	no
win2003unpatch.sainttest.local	info	User: TelnetClients (1002)	no
win2003unpatch.sainttest.local	info	User: localuser (1004)	no
win2003unpatch.sainttest.local	info	Windows service: Application Experience Lookup Service	no
win2003unpatch.sainttest.local	info	Windows service: Application Management	no
win2003unpatch.sainttest.local	info	Windows service: Automatic Updates	no
win2003unpatch.sainttest.local	info	Windows service: COM+ Event System	no
win2003unpatch.sainttest.local	info	Windows service: COM+ System Application	no
win2003unpatch.sainttest.local	info	Windows service: Computer Browser	no
win2003unpatch.sainttest.local	info	Windows service: Cryptographic Services	no
win2003unpatch.sainttest.local	info	Windows service: DCOM Server Process Launcher	no
win2003unpatch.sainttest.local	info	Windows service: DHCP Client	no
win2003unpatch.sainttest.local	info	Windows service: DNS Client	no
win2003unpatch.sainttest.local	info	Windows service: Distributed Link Tracking Client	no
win2003unpatch.sainttest.local	info	Windows service: Distributed Transaction Coordinator	no
win2003unpatch.sainttest.local	info	Windows service: Error Reporting Service	no
win2003unpatch.sainttest.local	info	Windows service: Event Log	no
win2003unpatch.sainttest.local	info	Windows service: Help and Support	no
win2003unpatch.sainttest.local	info	Windows service: IPSEC Services	no
win2003unpatch.sainttest.local	info	Windows service: Logical Disk Manager	no
win2003unpatch.sainttest.local	info	Windows service: Net Logon	no
win2003unpatch.sainttest.local	info	Windows service: Network Connections	no
win2003unpatch.sainttest.local	info	Windows service: Network Location Awareness (NLA)	no
win2003unpatch.sainttest.local	info	Windows service: Plug and Play	no
win2003unpatch.sainttest.local	info	Windows service: Print Spooler	no
win2003unpatch.sainttest.local	info	Windows service: Protected Storage	no
win2003unpatch.sainttest.local	info	Windows service: Remote Procedure Call (RPC)	no
win2003unpatch.sainttest.local	info	Windows service: Remote Registry	no
win2003unpatch.sainttest.local	info	Windows service: Secondary Logon	no
win2003unpatch.sainttest.local	info	Windows service: Security Accounts Manager	no
win2003unpatch.sainttest.local	info	Windows service: Server	no
win2003unpatch.sainttest.local	info	Windows service: Shell Hardware Detection	no
win2003unpatch.sainttest.local	info	Windows service: System Event Notification	no
win2003unpatch.sainttest.local	info	Windows service: TCP/IP NetBIOS Helper	no
win2003unpatch.sainttest.local	info	Windows service: Task Scheduler	no
win2003unpatch.sainttest.local	info	Windows service: Terminal Services	no

win2003unpatch.sainttest.local	info	Windows service: VMware Physical Disk Helper Service	no
win2003unpatch.sainttest.local	info	Windows service: VMware Tools Service	no
win2003unpatch.sainttest.local	info	Windows service: VMware Upgrade Helper	no
win2003unpatch.sainttest.local	info	Windows service: Windows Audio	no
win2003unpatch.sainttest.local	info	Windows service: Windows Management Instrumentation	no
win2003unpatch.sainttest.local	info	Windows service: Windows Time	no
win2003unpatch.sainttest.local	info	Windows service: Wireless Configuration	no
win2003unpatch.sainttest.local	info	Windows service: Workstation	no

5.0 Details

The following sections provide details on the specific vulnerabilities detected on each host.

5.1 win2003unpatch.sainttest.local

IP Address: 10.7.0.11
Scan time: Nov 01 11:44:30 2011

Host type: Windows Server 2003 SP2
Netbios Name: WIN2003UNPATCH

Microsoft Remote Desktop Protocol Denial of Service Vulnerability (MS11-065)

Severity: Critical Problem **CVE:** CVE-2011-1968

Impact

The absence of critical updates leads to the potential for denial of service or unauthorized access by attackers or malicious web sites.

The Problems and Resolutions

One or more of the following security updates is not installed on the target system. The resolution is to install the needed updates. This can be done either by following the links in the table, or by visiting the Windows Update service which will automatically determine which updates are needed for your system and help you install them. It is a good idea to make a backup of the system before installing an update, especially for service packs. After the system has been brought up to date, check Microsoft's web site regularly for new critical updates.

Note: The links below apply to the standard editions of Windows operating systems. If you are using a Terminal Server edition, a 64-bit edition, or a non-Intel edition which is not listed, consult the corresponding Microsoft Security Bulletins for patch information.

Update Name	Description	Fix	Bulletin
Microsoft Remote Desktop Protocol Denial of Service Vulnerability (MS11-065)	If the Remote Desktop Protocol is enabled but not patched, a maliciously-crafted sequence of RDP packets sent by a remote, unauthenticated attacker could cause a denial of service and possibly restart the target system. (CVE	**XP 32-bit SP3** 2570222 **XP 64-bit SP2** 2570222 **2003 32-bit SP2** 2570222 **2003 64-bit**	11-065

	2011-1968)	SP2 2570222 **2003 Itanium SP2** 2570222

Where can I read more about this?

For more information on critical updates, see the Windows critical update pages which are available for Windows 2000, Windows NT 4.0, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7.

Technical Details

Service: netbios
rdpwd.sys older than 2011-6-22

Microsoft Windows TCP/IP remote code execution vulnerability (MS09-048)

Severity: Critical Problem **CVE:** CVE-2006-2379 CVE-2008-4609 CVE-2009-1926

Impact

The absence of critical updates leads to the potential for denial of service or unauthorized access by attackers or malicious web sites.

The Problems and Resolutions

One or more of the following security updates is not installed on the target system. The resolution is to install the needed updates. This can be done either by following the links in the table, or by visiting the Windows Update service which will automatically determine which updates are needed for your system and help you install them. It is a good idea to make a backup of the system before installing an update, especially for service packs. After the system has been brought up to date, check Microsoft's web site regularly for new critical updates.

Note: The links below apply to the standard editions of Windows operating systems. If you are using a Terminal Server edition, a 64-bit edition, or a non-Intel edition which is not listed, consult the corresponding Microsoft Security Bulletins for patch information.

Update Name	Description	Fix	Bulletin
Microsoft Windows TCP/IP remote code execution vulnerability	Fixes several vulnerabilities in Transmission Control Protocol /Internet Protocol (TCP/IP) processing. The vulnerabilities could allow remote code execution if an attacker sent specially crafted TCP /IP packets over the network to a computer with a listening service. (CVE 2008-4609, CVE 2009-1925, CVE 2009-1926)	**2003:** 967723 **Vista:** 967723 **2008:** 967723	09-048

Where can I read more about this?

For more information on critical updates, see the Windows critical update pages which are available for Windows 2000, Windows NT 4.0, Windows XP, Windows Server 2003, Windows Vista, Windows Server

2008, and Windows 7.

Technical Details

Service: netbios
tcpip.sys older than 2009-8-14

Windows RPC authentication denial of service

Severity: Critical Problem **CVE:** CVE-2007-2228

Impact

The absence of critical updates leads to the potential for denial of service or unauthorized access by attackers or malicious web sites.

The Problems and Resolutions

One or more of the following security updates is not installed on the target system. The resolution is to install the needed updates. This can be done either by following the links in the table, or by visiting the Windows Update service which will automatically determine which updates are needed for your system and help you install them. It is a good idea to make a backup of the system before installing an update, especially for service packs. After the system has been brought up to date, check Microsoft's web site regularly for new critical updates.

Note: The links below apply to the standard editions of Windows operating systems. If you are using a Terminal Server edition, a 64-bit edition, or a non-Intel edition which is not listed, consult the corresponding Microsoft Security Bulletins for patch information.

Update Name	Description	Fix	Bulletin
Windows RPC Authentication denial of service	Fixes vulnerability in Windows RPC for Windows that allows for a denial of service to be caused in the RPC authentication. (CVE 2007-2228)	**2000:** 933729 **XP:** 933729 **2003:** 933729 **Vista:** 933729	07-058

Where can I read more about this?

For more information on critical updates, see the Windows critical update pages which are available for Windows 2000, Windows NT 4.0, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7.

Technical Details

Service: netbios
rpcrt4.dll older than 2007-7-7

Windows SMB Server Transaction Vulnerability

Severity: Critical Problem **CVE:** CVE-2011-0661

Impact

The absence of critical updates leads to the potential for denial of service or unauthorized access by attackers or malicious web sites.

The Problems and Resolutions

One or more of the following security updates is not installed on the target system. The resolution is to install the needed updates. This can be done either by following the links in the table, or by visiting the Windows Update service which will automatically determine which updates are needed for your system and help you install them. It is a good idea to make a backup of the system before installing an update, especially for service packs. After the system has been brought up to date, check Microsoft's web site regularly for new critical updates.

Note: The links below apply to the standard editions of Windows operating systems. If you are using a Terminal Server edition, a 64-bit edition, or a non-Intel edition which is not listed, consult the corresponding Microsoft Security Bulletins for patch information.

Update Name	Description	Fix	Bulletin
Windows SMB Server Transaction Vulnerability	Fixes multiple vulnerabilities in SMB server and SMB client which could allow remote code execution. (CVE 2011-0661)	**XP:** 2508429 (32-bit), 2508429 (64-bit) **2003:** 2508429 (32-bit), 2508429 (64-bit), **Vista:** 2508429 (32-bit), 2508429 (64-bit), **2008:** 2508429 (32-bit), 2508429 (64-bit), **Windows 7:** 2508429 (32-bit), 2508429 (64-bit), **Windows 7 SP1:** 2508429 (32-bit), 2508429 (64-bit), **2008 R2:** 2508429 (64-bit), **2008 R2 SP1:** 2508429 (64-bit)	11-020

Where can I read more about this?

For more information on critical updates, see the Windows critical update pages which are available for Windows 2000, Windows NT 4.0, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7.

Technical Details

Service: netbios
srv.sys older than 2011-2-16

Windows Server Service MS08-067 buffer overflow

Severity: Critical Problem **CVE:** CVE-2008-4250

Impact

The absence of critical updates leads to the potential for denial of service or unauthorized access by attackers or malicious web sites.

The Problems and Resolutions

One or more of the following security updates is not installed on the target system. The resolution is to install the needed updates. This can be done either by following the links in the table, or by visiting the Windows Update service which will automatically determine which updates are needed for your system and help you install them. It is a good idea to make a backup of the system before installing an update, especially for service packs. After the system has been brought up to date, check Microsoft's web site regularly for new critical updates.

Note: The links below apply to the standard editions of Windows operating systems. If you are using a Terminal Server edition, a 64-bit edition, or a non-Intel edition which is not listed, consult the corresponding Microsoft Security Bulletins for patch information.

Update Name	Description	Fix	Bulletin
Windows Server Service MS08-067 buffer overflow	Fixes a buffer overflow in the Windows Server service which could allow remote attackers to take complete control of the computer. (CVE 2008-4250)	**2000:** 958644 **XP:** 958644 **2003:** 958644 **Vista:** 958644 **2008:** 958644	08-067

Where can I read more about this?

For more information on critical updates, see the Windows critical update pages which are available for Windows 2000, Windows NT 4.0, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7.

Technical Details

Service: 445:TCP
NetprPathCompare returned 0

vulnerable version of SMB Server (MS10-012) dated 2007-2-17

Severity: Critical Problem

CVE: CVE-2010-0020 CVE-2010-0021 CVE-2010-0022 CVE-2010-0231

Impact

The absence of critical updates leads to the potential for denial of service or unauthorized access by attackers or malicious web sites.

The Problems and Resolutions

One or more of the following security updates is not installed on the target system. The resolution is to install the needed updates. This can be done either by following the links in the table, or by visiting the Windows Update service which will automatically determine which updates are needed for your system and help you install them. It is a good idea to make a backup of the system before installing an update, especially for service packs. After the system has been brought up to date, check Microsoft's web site regularly for new

critical updates.

Note: The links below apply to the standard editions of Windows operating systems. If you are using a Terminal Server edition, a 64-bit edition, or a non-Intel edition which is not listed, consult the corresponding Microsoft Security Bulletins for patch information.

Update Name	Description	Fix	Bulletin
Multiple vulnerabilities (MS10-012)	Fixes 4 vulnerabilities announced in Microsoft bulletin MS10-012, the most critical of which could allow remote code execution. The vulnerabilities are due to weak entropy used in encryption, bounds checking on path names, and null pointers. (CVE 2010-0020 CVE 2010-0021 CVE 2010-0022 CVE 2010-0231)	**2000 (all versions):** 971468 **XP:** 971468 **2003 (all versions):** 971468 **Vista (all versions):** 971468 **Windows 7 (all versions):** 971468 **2008 (all versions):** 971468	10-007

Where can I read more about this?

For more information on critical updates, see the Windows critical update pages which are available for Windows 2000, Windows NT 4.0, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7.

Technical Details

Service: netbios
srv.sys older than 2009-12-1

Internet Explorer 6 vulnerable version, mshtml.dll dated 2007-2-17

Severity: Area of Concern

CVE: CVE-2007-0218 CVE-2007-0942 CVE-2007-0944 CVE-2007-0945 CVE-2007-1091 CVE-2007-1750 CVE-2007-1751 CVE-2007-2216 CVE-2007-2221 CVE-2007-2222 CVE-2007-3027 CVE-2007-3041 CVE-2007-3091 CVE-2007-3826 CVE-2007-3892 CVE-2007-3893 CVE-2007-3902 CVE-2007-3903 CVE-2007-4790 CVE-2007-5158 CVE-2007-5344 CVE-2007-5347 CVE-2008-0076 CVE-2008-0077 CVE-2008-0078 CVE-2008-1085 CVE-2008-1442 CVE-2008-1544 CVE-2008-2254 CVE-2008-2255 CVE-2008-2256 CVE-2008-2257 CVE-2008-2258 CVE-2008-2259

CVE-2008-2947 CVE-2008-3472
CVE-2008-3473 CVE-2008-3474
CVE-2008-3475 CVE-2008-3476
CVE-2008-4261 CVE-2008-4844
CVE-2009-0550 CVE-2009-0551
CVE-2009-0552 CVE-2009-0553
CVE-2009-0554 CVE-2009-1140
CVE-2009-1141 CVE-2009-1528
CVE-2009-1547 CVE-2009-1917
CVE-2009-1918 CVE-2009-1919
CVE-2009-2493 CVE-2009-2529
CVE-2009-2530 CVE-2009-2531
CVE-2009-3672 CVE-2010-0244
CVE-2010-0247 CVE-2010-0248
CVE-2010-0249 CVE-2010-0255
CVE-2010-0267 CVE-2010-0488
CVE-2010-0489 CVE-2010-0490
CVE-2010-0491 CVE-2010-0494
CVE-2010-0805 CVE-2010-0806
CVE-2010-0808 CVE-2010-1258
CVE-2010-1259 CVE-2010-1262
CVE-2010-2556 CVE-2010-2557
CVE-2010-2558 CVE-2010-2560
CVE-2010-3325 CVE-2010-3326
CVE-2010-3327 CVE-2010-3328
CVE-2010-3330 CVE-2010-3331
CVE-2010-3340 CVE-2010-3342
CVE-2010-3343 CVE-2010-3346
CVE-2010-3348 CVE-2010-3962
CVE-2010-3971 CVE-2011-0035
CVE-2011-0036 CVE-2011-0094
CVE-2011-0346 CVE-2011-1244
CVE-2011-1245 CVE-2011-1250
CVE-2011-1254 CVE-2011-1255
CVE-2011-1256 CVE-2011-1257
CVE-2011-1258 CVE-2011-1261
CVE-2011-1345 CVE-2011-1960
CVE-2011-1961 CVE-2011-1962
CVE-2011-1964 CVE-2011-1993
CVE-2011-1995 CVE-2011-1996
CVE-2011-1997 CVE-2011-2000
CVE-2011-2001 CVE-2011-2383

Impact

A remote attacker could execute arbitrary commands on a client system when the client browses to a malicious web site hosted by the attacker.

Resolution

To use Internet Explorer securely, take the following steps:

(The vulnerabilities in IE 8, Beta 1 have not yet been patched)

(The response splitting and smuggling related to setRequestHeader() has not yet been patched)

(The file focus stealing vulnerability has not yet been patched)

(The stack overflow vulnerability has not yet been patched.)

(The document.open spoofing vulnerability has not yet been patched.)

(The CSS parser vulnerability has not yet been patched.)

- Install the appropriate cumulative patch for your version of Internet Explorer as outlined in Microsoft Security Bulletins 07-009, 07-061, 08-022, 08-032, 08-052, 10-002, 11-031, 11-052, and 11-081.
- Fix the Security Zone Bypass vulnerability (CVE-2010-0255) as described in Microsoft Security Advisory (980088)
- Prevent WPAD proxy server interception as described in Microsoft Knowledge Base Article 934864
- Disable the Javaprxy.dll object
- Disable the ADODB.Stream object
- Disable the Shell.Explorer object

Instructions for disabling the ADODB.Stream object can be found in Microsoft Knowledge Base Article 870669.

To disable the Shell.Explorer object, set the following registry value:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX
Compatibility\{8856F961-340A-11D0-A96B-00C04FD705A2}
Compatibility Flags = 400 (type dword, radix hex)
```

To disable the Javaprxy.dll object, install the update referenced in Microsoft Security Bulletin 05-037.

Where can I read more about this?

For more information on all Internet Explorer security fixes, see the Internet Explorer Critical Updates page.

The Security Zone Bypass vulnerability (CVE-2010-0255) was reported in Microsoft Security Advisory (980088).

The CSS parser vulnerability (CVE-2010-3971) was reported in Microsoft Security Advisory (2488013).

For more information on specific vulnerabilities, see Microsoft Security Bulletins 03-004, 03-015, 03-020, 03-032, 03-040, 03-048, 04-004, 04-025, 04-038, 04-040, 05-014, 05-020, 05-025, 05-037, 05-038, 05-052, 05-054, 06-004, 06-013, 06-021, 06-023, 06-042, 06-055, 06-067, 06-072, 07-004, 07-009, 07-016, 07-027, 07-033, 07-045, 07-050, 07-057, 07-061, 07-069, 08-010, 08-022, 08-023, 08-024, 08-031, 08-032, 08-045, 08-052, 08-058, 08-073, 08-078, 09-002, 09-014, 09-019, 09-034, 09-045, 09-054, 09-072, 10-002, 10-018, 10-035, 10-053, 10-071, 10-090, 11-003, 11-018, 11-031, 11-052, 11-050, 11-057, and 11-081.

Also see CERT advisories CA-2003-22, TA04-033A, TA04-163A, TA04-212A, TA04-293A, TA04-315A, TA04-336A, TA05-165A, TA05-221A, and US-CERT Vulnerability Note VU#378604.

The IE 8, Beta 1 vulnerabilities were reported in Bugtraq ID 28580 and Bugtraq ID 28581.

The `setRequestHeader()` related vulnerabilities were reported in Secunia Advisory SA29453.

The document.open spoofing vulnerability was reported in Secunia Advisory SA26069.

More information on the race condition building DOM objects vulnerability was reported in Secunia Advisory SA25564.

More information on the Unload JavaScript vulnerabilities may be found at Bugtraq ID 22678 and Bugtraq ID 22680.

Unfixed variants of the drag and drop vulnerability and the Shell.Explorer object were discussed in NTBugtraq and Full Disclosure.

Technical Details

Service: netbios
mshtml.dll older than 2011-9-3

Internet Explorer VBScript and JScript decoding vulnerability

Severity: Area of Concern **CVE:** CVE-2008-0083

Impact

A remote attacker could execute arbitrary commands on a client system when the client browses to a malicious web site hosted by the attacker.

Resolution

To use Internet Explorer securely, take the following steps:

(The vulnerabilities in IE 8, Beta 1 have not yet been patched)

(The response splitting and smuggling related to setRequestHeader() has not yet been patched)

(The file focus stealing vulnerability has not yet been patched)

(The stack overflow vulnerability has not yet been patched.)

(The document.open spoofing vulnerability has not yet been patched.)

- Install the appropriate cumulative patch for your version of Internet Explorer as outlined in Microsoft Security Bulletins 07-009, 07-061, 08-022, 08-032, 08-052, 10-002, 11-031, 11-052, and 11-081.
- Fix the Security Zone Bypass vulnerability (CVE-2010-0255) as described in Microsoft Security Advisory (980088)
- Prevent WPAD proxy server interception as described in Microsoft Knowledge Base Article 934864
- Disable the Javaprxy.dll object
- Disable the ADODB.Stream object
- Disable the Shell.Explorer object

Instructions for disabling the ADODB.Stream object can be found in Microsoft Knowledge Base Article 870669.

To disable the Shell.Explorer object, set the following registry value:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX
Compatibility\{8856F961-340A-11D0-A96B-00C04FD705A2}
Compatibility Flags = 400 (type dword, radix hex)
```

To disable the Javaprxy.dll object, install the update referenced in Microsoft Security Bulletin 05-037.

Where can I read more about this?

For more information on all Internet Explorer security fixes, see the Internet Explorer Critical Updates page.

For more information on specific vulnerabilities, see Microsoft Security Bulletins 03-004, 03-015, 03-020, 03-032, 03-040, 03-048, 04-004, 04-025, 04-038, 04-040, 05-014, 05-020, 05-025, 05-037, 05-038, 05-052, 05-054, 06-004, 06-013, 06-021, 06-023, 06-042, 06-055, 06-067, 06-072, 07-004, 07-009, 07-016, 07-027, 07-033, 07-045, 07-050, 07-057, 07-061, 07-069, 08-010, 08-022, 08-023, 08-024, 08-031, 08-032, 08-045, 08-052, 08-058, 08-073, 08-078, 09-002, 09-014, 09-019, 09-034, 09-045, 09-054, 09-072, 10-002, 10-018, 10-035, 10-053, 10-071, 10-090, 11-003, 11-018, 11-031, 11-052, 11-050, 11-057, and 11-081.

Also see CERT advisories CA-2003-22, TA04-033A, TA04-163A, TA04-212A, TA04-293A, TA04-315A, TA04-336A, TA05-165A, TA05-221A, and US-CERT Vulnerability Note VU#378604.

The IE 8, Beta 1 vulnerabilities were reported in Bugtraq ID 28580 and Bugtraq ID 28581.

Unfixed variants of the drag and drop vulnerability and the Shell.Explorer object were discussed in NTBugtraq and Full Disclosure.

Technical Details

Service: netbios
jscript.dll older than 2007-12-12

Internet Explorer VBScript and JScript memory reallocation vulnerability (MS11-031)

Severity: Area of Concern **CVE:** CVE-2011-0663

Impact

A remote attacker could execute arbitrary commands on a client system when the client browses to a malicious web site hosted by the attacker.

Resolution

To use Internet Explorer securely, take the following steps:

(The vulnerabilities in IE 8, Beta 1 have not yet been patched)

(The response splitting and smuggling related to setRequestHeader() has not yet been patched)

(The file focus stealing vulnerability has not yet been patched)

(The stack overflow vulnerability has not yet been patched.)

(The document.open spoofing vulnerability has not yet been patched.)

- Install the appropriate cumulative patch for your version of Internet Explorer as outlined in Microsoft Security Bulletins 07-009, 07-061, 08-022, 08-032, 08-052, 10-002, 11-031, 11-052, and 11-081.
- Fix the Security Zone Bypass vulnerability (CVE-2010-0255) as described in Microsoft Security Advisory (980088)
- Prevent WPAD proxy server interception as described in Microsoft Knowledge Base Article 934864
- Disable the Javaprxy.dll object
- Disable the ADODB.Stream object
- Disable the Shell.Explorer object

Instructions for disabling the ADODB.Stream object can be found in Microsoft Knowledge Base Article 870669.

To disable the Shell.Explorer object, set the following registry value:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX
Compatibility\{8856F961-340A-11D0-A96B-00C04FD705A2}
Compatibility Flags = 400 (type dword, radix hex)
```

To disable the Javaprxy.dll object, install the update referenced in Microsoft Security Bulletin 05-037.

Where can I read more about this?

For more information on all Internet Explorer security fixes, see the Internet Explorer Critical Updates page.

For more information on specific vulnerabilities, see Microsoft Security Bulletins 03-004, 03-015, 03-020, 03-032, 03-040, 03-048, 04-004, 04-025, 04-038, 04-040, 05-014, 05-020, 05-025, 05-037, 05-038, 05-052, 05-054, 06-004, 06-013, 06-021, 06-023, 06-042, 06-055, 06-067, 06-072, 07-004, 07-009, 07-016, 07-027, 07-033, 07-045, 07-050, 07-057, 07-061, 07-069, 08-010, 08-022, 08-023, 08-024, 08-031, 08-032, 08-045, 08-052, 08-058, 08-073, 08-078, 09-002, 09-014, 09-019, 09-034, 09-045, 09-054, 09-072, 10-002, 10-018, 10-035, 10-053, 10-071, 10-090, 11-003, 11-018, 11-031, 11-052, 11-050, 11-057, and 11-081.

Also see CERT advisories CA-2003-22, TA04-033A, TA04-163A, TA04-212A, TA04-293A, TA04-315A, TA04-336A, TA05-165A, TA05-221A, and US-CERT Vulnerability Note VU#378604.

The IE 8, Beta 1 vulnerabilities were reported in Bugtraq ID 28580 and Bugtraq ID 28581.

Unfixed variants of the drag and drop vulnerability and the Shell.Explorer object were discussed in NTBugtraq and Full Disclosure.

Technical Details

Service: netbios
jscript.dll older than 2011-2-14

Internet Explorer vulnerable VML version dated 2007-2-17

Severity: Area of Concern **CVE:** CVE-2007-1749 CVE-2011-1266

Impact

A remote attacker could execute arbitrary commands on a client system when the client browses to a malicious web site hosted by the attacker.

Resolution

To use Internet Explorer securely, take the following steps:

(The vulnerabilities in IE 8, Beta 1 have not yet been patched)

(The response splitting and smuggling related to setRequestHeader() has not yet been patched)

(The file focus stealing vulnerability has not yet been patched)

(The stack overflow vulnerability has not yet been patched.)

(The document.open spoofing vulnerability has not yet been patched.)

- Install the appropriate cumulative patch for your version of Internet Explorer as outlined in Microsoft Security Bulletins 07-009, 07-061, 08-022, 08-032, 08-052, 10-002, 11-031, 11-052, and 11-081.
- Fix the Security Zone Bypass vulnerability (CVE-2010-0255) as described in Microsoft Security Advisory (980088)
- Prevent WPAD proxy server interception as described in Microsoft Knowledge Base Article 934864
- Disable the Javaprxy.dll object
- Disable the ADODB.Stream object
- Disable the Shell.Explorer object

Instructions for disabling the ADODB.Stream object can be found in Microsoft Knowledge Base Article 870669.

To disable the Shell.Explorer object, set the following registry value:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX
Compatibility\{8856F961-340A-11D0-A96B-00C04FD705A2}
Compatibility Flags = 400 (type dword, radix hex)
```

To disable the Javaprxy.dll object, install the update referenced in Microsoft Security Bulletin 05-037.

Where can I read more about this?

For more information on all Internet Explorer security fixes, see the Internet Explorer Critical Updates page.

For more information on specific vulnerabilities, see Microsoft Security Bulletins 03-004, 03-015, 03-020, 03-032, 03-040, 03-048, 04-004, 04-025, 04-038, 04-040, 05-014, 05-020, 05-025, 05-037, 05-038, 05-052, 05-054, 06-004, 06-013, 06-021, 06-023, 06-042, 06-055, 06-067, 06-072, 07-004, 07-009, 07-016, 07-027, 07-033, 07-045, 07-050, 07-057, 07-061, 07-069, 08-010, 08-022, 08-023, 08-024, 08-031, 08-032, 08-045, 08-052, 08-058, 08-073, 08-078, 09-002, 09-014, 09-019, 09-034, 09-045, 09-054, 09-072, 10-002, 10-018, 10-035, 10-053, 10-071, 10-090, 11-003, 11-018, 11-031, 11-052, 11-050, 11-057, and 11-081.

Also see CERT advisories CA-2003-22, TA04-033A, TA04-163A, TA04-212A, TA04-293A, TA04-315A, TA04-336A, TA05-165A, TA05-221A, and US-CERT Vulnerability Note VU#378604.

The IE 8, Beta 1 vulnerabilities were reported in Bugtraq ID 28580 and Bugtraq ID 28581.

Unfixed variants of the drag and drop vulnerability and the Shell.Explorer object were discussed in NTBugtraq and Full Disclosure.

Technical Details

Service: netbios
vgx.dll older than 2011-4-27

Jscript.dll buffer overflow vulnerability

Severity: Area of Concern **CVE:** CVE-2009-1920

Impact

A remote attacker could execute arbitrary commands on a client system when the client browses to a malicious web site hosted by the attacker.

Resolution

To use Internet Explorer securely, take the following steps:

(The vulnerabilities in IE 8, Beta 1 have not yet been patched)

(The response splitting and smuggling related to setRequestHeader() has not yet been patched)

(The file focus stealing vulnerability has not yet been patched)

(The stack overflow vulnerability has not yet been patched.)

(The document.open spoofing vulnerability has not yet been patched.)

- Install the appropriate cumulative patch for your version of Internet Explorer as outlined in Microsoft Security Bulletins 07-009, 07-061, 08-022, 08-032, 08-052, 10-002, 11-031, 11-052, and 11-081.
- Fix the Security Zone Bypass vulnerability (CVE-2010-0255) as described in Microsoft Security Advisory (980088)
- Prevent WPAD proxy server interception as described in Microsoft Knowledge Base Article 934864
- Disable the Javaprxy.dll object
- Disable the ADODB.Stream object
- Disable the Shell.Explorer object

Instructions for disabling the ADODB.Stream object can be found in Microsoft Knowledge Base Article 870669.

To disable the Shell.Explorer object, set the following registry value:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX
Compatibility\{8856F961-340A-11D0-A96B-00C04FD705A2}
Compatibility Flags = 400 (type dword, radix hex)
```

To disable the Javaprxy.dll object, install the update referenced in Microsoft Security Bulletin 05-037.

Where can I read more about this?

For more information on all Internet Explorer security fixes, see the Internet Explorer Critical Updates page.

For more information on specific vulnerabilities, see Microsoft Security Bulletins 03-004, 03-015, 03-020,

03-032, 03-040, 03-048, 04-004, 04-025, 04-038, 04-040, 05-014, 05-020, 05-025, 05-037, 05-038, 05-052, 05-054, 06-004, 06-013, 06-021, 06-023, 06-042, 06-055, 06-067, 06-072, 07-004, 07-009, 07-016, 07-027, 07-033, 07-045, 07-050, 07-057, 07-061, 07-069, 08-010, 08-022, 08-023, 08-024, 08-031, 08-032, 08-045, 08-052, 08-058, 08-073, 08-078, 09-002, 09-014, 09-019, 09-034, 09-045, 09-054, 09-072, 10-002, 10-018, 10-035, 10-053, 10-071, 10-090, 11-003, 11-018, 11-031, 11-052, 11-050, 11-057, and 11-081.

Also see CERT advisories CA-2003-22, TA04-033A, TA04-163A, TA04-212A, TA04-293A, TA04-315A, TA04-336A, TA05-165A, TA05-221A, and US-CERT Vulnerability Note VU#378604.

The IE 8, Beta 1 vulnerabilities were reported in Bugtraq ID 28580 and Bugtraq ID 28581.

Unfixed variants of the drag and drop vulnerability and the Shell.Explorer object were discussed in NTBugtraq and Full Disclosure.

Technical Details

Service: netbios
jscript.dll older than 2009-6-1

sapi.dll ActiveX vulnerability

Severity: Area of Concern **CVE:** CVE-2007-0675

Impact

A remote attacker could execute arbitrary commands on a client system when the client browses to a malicious web site hosted by the attacker.

Resolution

To use Internet Explorer securely, take the following steps:

(The vulnerabilities in IE 8, Beta 1 have not yet been patched)

(The response splitting and smuggling related to setRequestHeader() has not yet been patched)

(The file focus stealing vulnerability has not yet been patched)

(The stack overflow vulnerability has not yet been patched.)

(The document.open spoofing vulnerability has not yet been patched.)

- Install the appropriate cumulative patch for your version of Internet Explorer as outlined in Microsoft Security Bulletins 07-009, 07-061, 08-022, 08-032, 08-052, 10-002, 11-031, 11-052, and 11-081.
- Fix the Security Zone Bypass vulnerability (CVE-2010-0255) as described in Microsoft Security Advisory (980088)
- Prevent WPAD proxy server interception as described in Microsoft Knowledge Base Article 934864
- Disable the Javaprxy.dll object
- Disable the ADODB.Stream object
- Disable the Shell.Explorer object

Instructions for disabling the ADODB.Stream object can be found in Microsoft Knowledge Base Article 870669.

To disable the Shell.Explorer object, set the following registry value:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX
Compatibility\{8856F961-340A-11D0-A96B-00C04FD705A2}
Compatibility Flags = 400 (type dword, radix hex)
```

To disable the Javaprxy.dll object, install the update referenced in Microsoft Security Bulletin 05-037.

Where can I read more about this?

For more information on all Internet Explorer security fixes, see the Internet Explorer Critical Updates page.

For more information on specific vulnerabilities, see Microsoft Security Bulletins 03-004, 03-015, 03-020, 03-032, 03-040, 03-048, 04-004, 04-025, 04-038, 04-040, 05-014, 05-020, 05-025, 05-037, 05-038, 05-052, 05-054, 06-004, 06-013, 06-021, 06-023, 06-042, 06-055, 06-067, 06-072, 07-004, 07-009, 07-016, 07-027, 07-033, 07-045, 07-050, 07-057, 07-061, 07-069, 08-010, 08-022, 08-023, 08-024, 08-031, 08-032, 08-045, 08-052, 08-058, 08-073, 08-078, 09-002, 09-014, 09-019, 09-034, 09-045, 09-054, 09-072, 10-002, 10-018, 10-035, 10-053, 10-071, 10-090, 11-003, 11-018, 11-031, 11-052, 11-050, 11-057, and 11-081.

Also see CERT advisories CA-2003-22, TA04-033A, TA04-163A, TA04-212A, TA04-293A, TA04-315A, TA04-336A, TA05-165A, TA05-221A, and US-CERT Vulnerability Note VU#378604.

The IE 8, Beta 1 vulnerabilities were reported in Bugtraq ID 28580 and Bugtraq ID 28581.

Unfixed variants of the drag and drop vulnerability and the Shell.Explorer object were discussed in NTBugtraq and Full Disclosure.

Technical Details

Service: netbios
HKLM\SOFTWARE\Microsoft\Internet Explorer\ActiveX Compatibility\{47206204-5eca-11d2-960f-00c04f8ee628}\Compatibility Flags is not 0x400 or HKLM\SOFTWARE\Microsoft\Internet Explorer\ActiveX Compatibility\{3bee4890-4fe9-4a37-8c1e-5e7e12791c1f}\Compatibility Flags is not 0x400

Macrovision SafeDisc driver local privilege elevation

Severity: Area of Concern **CVE:** CVE-2007-5587

Impact

A vulnerability in Macrovision SafeDisc allows arbitrary code to be executed by local users.

Resolution

The `secdrv.sys` file should be updated through either Macrovision or Microsoft (XP/2003).

Where can I read more about this?

The `secdrv.sys` local privilege elevation was reported in MS07-067.

Technical Details

Service: netbios
secdrv.sys older than 2007-11-10

Information disclosure vulnerability in .NET Framework

Severity: Area of Concern **CVE:** CVE-2011-1978

Impact

On a workstation, a remote attacker could execute arbitrary commands when a user opens a specially crafted web page. On a server, a remote attacker could gain unauthorized access to configuration files.

Resolution

Install the patch referenced in Microsoft Security Bulletins:

- 10-041 (.NET Framework 1.0, 1.1, 2.0, 3.5)
- 11-039 (Silverlight 4)
- 11-069 (.NET Framework 2.0, 3.5, 4.0)
- 11-044 (.NET Framework 2.0, 3.5, 4.0)
- 11-066 (.NET Framework 3.5, 4.0)
- 11-078 (.NET Framework 1.0, 1.1, 2.0, 3.5, 4.0, Silverlight 4)

Where can I read more about this?

For more information, see Microsoft Security Bulletins 07-040, 09-036, 09-061, 10-041, 10-060, 11-028, 11-039, 11-044, 11-066, 11-069, and 11-078.

Technical Details

Service: netbios
system.dll older than 2011-4-26

MS11-028 Vulnerability in .NET Framework Could Allow Remote Code Execution

Severity: Area of Concern **CVE:** CVE-2010-3958

Impact

On a workstation, a remote attacker could execute arbitrary commands when a user opens a specially crafted web page. On a server, a remote attacker could gain unauthorized access to configuration files.

Resolution

Install the patch referenced in Microsoft Security Bulletins:

- 10-041 (.NET Framework 1.0, 1.1, 2.0, 3.5)
- 11-039 (Silverlight 4)
- 11-069 (.NET Framework 2.0, 3.5, 4.0)
- 11-044 (.NET Framework 2.0, 3.5, 4.0)
- 11-066 (.NET Framework 3.5, 4.0)
- 11-078 (.NET Framework 1.0, 1.1, 2.0, 3.5, 4.0, Silverlight 4)

Where can I read more about this?

For more information, see Microsoft Security Bulletins 07-040, 09-036, 09-061, 10-041, 10-060, 11-028, 11-039, 11-044, 11-066, 11-069, and 11-078.

Technical Details

Service: netbios
mscorlib.dll older than 2010-10-28

MS11-039 Vulnerability in .NET Framework Could Allow Remote Code Execution

Severity: Area of Concern **CVE:** CVE-2011-0664

Impact

On a workstation, a remote attacker could execute arbitrary commands when a user opens a specially crafted web page. On a server, a remote attacker could gain unauthorized access to configuration files.

Resolution

Install the patch referenced in Microsoft Security Bulletins:

- 10-041 (.NET Framework 1.0, 1.1, 2.0, 3.5)
- 11-039 (Silverlight 4)
- 11-069 (.NET Framework 2.0, 3.5, 4.0)
- 11-044 (.NET Framework 2.0, 3.5, 4.0)
- 11-066 (.NET Framework 3.5, 4.0)
- 11-078 (.NET Framework 1.0, 1.1, 2.0, 3.5, 4.0, Silverlight 4)

Where can I read more about this?

For more information, see Microsoft Security Bulletins 07-040, 09-036, 09-061, 10-041, 10-060, 11-028, 11-039, 11-044, 11-066, 11-069, and 11-078.

Technical Details

Service: netbios
system.dll older than 2011-1-16

MS11-044 Vulnerability in .NET Framework Could Allow Remote Code Execution

Severity: Area of Concern **CVE:** CVE-2011-1271

Impact

On a workstation, a remote attacker could execute arbitrary commands when a user opens a specially crafted web page. On a server, a remote attacker could gain unauthorized access to configuration files.

Resolution

Install the patch referenced in Microsoft Security Bulletins:

- 10-041 (.NET Framework 1.0, 1.1, 2.0, 3.5)
- 11-039 (Silverlight 4)
- 11-069 (.NET Framework 2.0, 3.5, 4.0)

- 11-044 (.NET Framework 2.0, 3.5, 4.0)
- 11-066 (.NET Framework 3.5, 4.0)
- 11-078 (.NET Framework 1.0, 1.1, 2.0, 3.5, 4.0, Silverlight 4)

Where can I read more about this?

For more information, see Microsoft Security Bulletins 07-040, 09-036, 09-061, 10-041, 10-060, 11-028, 11-039, 11-044, 11-066, 11-069, and 11-078.

Technical Details

Service: netbios
mscorlib.dll older than 2011-3-23

MS11-078 Vulnerability in .NET Framework Could Allow Remote Code Execution

Severity: Area of Concern **CVE:** CVE-2011-1253

Impact

On a workstation, a remote attacker could execute arbitrary commands when a user opens a specially crafted web page. On a server, a remote attacker could gain unauthorized access to configuration files.

Resolution

Install the patch referenced in Microsoft Security Bulletins:

- 10-041 (.NET Framework 1.0, 1.1, 2.0, 3.5)
- 11-039 (Silverlight 4)
- 11-069 (.NET Framework 2.0, 3.5, 4.0)
- 11-044 (.NET Framework 2.0, 3.5, 4.0)
- 11-066 (.NET Framework 3.5, 4.0)
- 11-078 (.NET Framework 1.0, 1.1, 2.0, 3.5, 4.0, Silverlight 4)

Where can I read more about this?

For more information, see Microsoft Security Bulletins 07-040, 09-036, 09-061, 10-041, 10-060, 11-028, 11-039, 11-044, 11-066, 11-069, and 11-078.

Technical Details

Service: netbios
mscorlib.dll older than 2011-7-7

Microsoft .NET CLR virtual method delegate vulnerability

Severity: Area of Concern **CVE:** CVE-2010-1898

Impact

On a workstation, a remote attacker could execute arbitrary commands when a user opens a specially crafted web page. On a server, a remote attacker could gain unauthorized access to configuration files.

Resolution

Install the patch referenced in Microsoft Security Bulletins:

- 10-041 (.NET Framework 1.0, 1.1, 2.0, 3.5)
- 11-039 (Silverlight 4)
- 11-069 (.NET Framework 2.0, 3.5, 4.0)
- 11-044 (.NET Framework 2.0, 3.5, 4.0)
- 11-066 (.NET Framework 3.5, 4.0)
- 11-078 (.NET Framework 1.0, 1.1, 2.0, 3.5, 4.0, Silverlight 4)

Where can I read more about this?

For more information, see Microsoft Security Bulletins 07-040, 09-036, 09-061, 10-041, 10-060, 11-028, 11-039, 11-044, 11-066, 11-069, and 11-078.

Technical Details

Service: netbios
mscorlib.dll older than 2010-5-9

Microsoft .NET Common Language Runtime Could Allow Remote Code Execution

Severity: Area of Concern **CVE:** CVE-2009-0090 CVE-2009-0091 CVE-2009-2497

Impact

On a workstation, a remote attacker could execute arbitrary commands when a user opens a specially crafted web page. On a server, a remote attacker could gain unauthorized access to configuration files.

Resolution

Install the patch referenced in Microsoft Security Bulletins:

- 10-041 (.NET Framework 1.0, 1.1, 2.0, 3.5)
- 11-039 (Silverlight 4)
- 11-069 (.NET Framework 2.0, 3.5, 4.0)
- 11-044 (.NET Framework 2.0, 3.5, 4.0)
- 11-066 (.NET Framework 3.5, 4.0)
- 11-078 (.NET Framework 1.0, 1.1, 2.0, 3.5, 4.0, Silverlight 4)

Where can I read more about this?

For more information, see Microsoft Security Bulletins 07-040, 09-036, 09-061, 10-041, 10-060, 11-028, 11-039, 11-044, 11-066, 11-069, and 11-078.

Technical Details

Service: netbios
mscorlib.dll older than 2008-5-27

Microsoft .NET Framework Could Allow Tampering

Severity: Area of Concern **CVE:** CVE-2009-0217

Impact

On a workstation, a remote attacker could execute arbitrary commands when a user opens a specially crafted web page. On a server, a remote attacker could gain unauthorized access to configuration files.

Resolution

Install the patch referenced in Microsoft Security Bulletins:

- 10-041 (.NET Framework 1.0, 1.1, 2.0, 3.5)
- 11-039 (Silverlight 4)
- 11-069 (.NET Framework 2.0, 3.5, 4.0)
- 11-044 (.NET Framework 2.0, 3.5, 4.0)
- 11-066 (.NET Framework 3.5, 4.0)
- 11-078 (.NET Framework 1.0, 1.1, 2.0, 3.5, 4.0, Silverlight 4)

Where can I read more about this?

For more information, see Microsoft Security Bulletins 07-040, 09-036, 09-061, 10-041, 10-060, 11-028, 11-039, 11-044, 11-066, 11-069, and 11-078.

Technical Details

Service: netbios
System.Security.dll older than 2010-3-3

Microsoft outlook ATL vulnerability (MS09-037)

Severity: Area of Concern **CVE:** CVE-2008-0015 CVE-2008-0020 CVE-2009-0901 CVE-2009-2493 CVE-2009-2494

Impact

A vulnerability could allow remote attackers to bypass security restrictions and execute remote code.

Resolution

Apply the appropriate patch as indicated in Microsoft Security Bulletin MS10-030.

Where can I read more about this?

Technical Details

Service: netbios
msoe.dll older than 2009-7-8

Outlook Express Could Allow Remote Code Execution (MS10-030)

Severity: Area of Concern **CVE:** CVE-2010-0816

Impact

A vulnerability could allow remote attackers to bypass security restrictions and execute remote code.

Resolution

Apply the appropriate patch as indicated in Microsoft Security Bulletin MS10-030.

Where can I read more about this?

Technical Details

Service: netbios
msoe.dll older than 2010-1-31

Windows MHTML protocol handler vulnerability

Severity: Area of Concern **CVE:** CVE-2008-1448

Impact

A vulnerability could allow remote attackers to bypass security restrictions and execute remote code.

Resolution

Apply the appropriate patch as indicated in Microsoft Security Bulletin MS10-030.

Where can I read more about this?

The MHTML protocol handler component vulnerability was reported in Microsoft Security Bulletin MS08-048.

Technical Details

Service: registry
SOFTWARE\Microsoft\Updates\Windows Server 2003\SP3\KB951066 not found

fraudulent Comodo certificates not in disallowed store

Severity: Area of Concern

Impact

Vulnerability on all supported releases of Microsoft Windows may be used to conduct spoofing attacks, perform phishing attacks, or perform man-in-the-middle attacks against all Web browser users including users of Internet Explorer.

Resolution

For Fraudulent Comodo certificates, Microsoft has issued an update to address this issue.

Where can I read more about this?

The Fraudulent Comodo certificates vulnerability was reported in Microsoft Security Advisory 2524375.

Technical Details

Service: registry
SOFTWARE\Microsoft\SystemCertificates\Disallowed\Certificates\CEA586B2CE593EC7D939898337C5781

4708AB2BE not found

fraudulent DigiNotar certificates not in disallowed store

Severity: Area of Concern

Impact

Vulnerability on all supported releases of Microsoft Windows may be used to conduct spoofing attacks, perform phishing attacks, or perform man-in-the-middle attacks against all Web browser users including users of Internet Explorer.

Resolution

For Fraudulent DigiNotar certificates, Microsoft has issued an update to address this issue.

Where can I read more about this?

The Fraudulent DigiNotar certificates vulnerability was reported in Microsoft Security Advisory 2607712.

Technical Details

Service: registry
SOFTWARE\Microsoft\SystemCertificates\Disallowed\Certificates\367D4B3B4FCBBC0B767B2EC0CDB2A36EAB71A4EB and
SOFTWARE\Microsoft\SystemCertificates\Disallowed\Certificates\40AA38731BD189F9CDB5B9DC35E2136F38777AF4 not found

Telnet Authentication Reflection

Severity: Area of Concern **CVE:** CVE-2009-1930

Impact

A remote user could execute arbitrary commands on the server, cause the telnet server to stop responding, or gain information that could be used in an attempt to find Guest accounts.

Resolution

Apply the patches referenced in Microsoft Security Bulletins 09-042, 01-031 and 02-004.

Where can I read more about this?

For more information, see Microsoft Security Bulletins 09-042, 01-031 and 02-004.

Technical Details

Service: netbios
telnet.exe older than 2009-6-8

Insecure Library Loading in Outlook Express WAB.EXE Could Allow Remote Code Execution

Severity: Area of Concern **CVE:** CVE-2010-3147

Impact

There are several vulnerabilities in e-mail clients, the most severe of which could allow a remote attacker to execute arbitrary commands by sending a specially crafted e-mail message.

Resolution

Install the patches referenced in Microsoft Security Bulletin 01-038 and 08-015 for Outlook. Also, for Outlook 2002, install the patches referenced in 02-067, 03-003, and 04-009, or Office XP service pack 3.

For Outlook Express:
Install the patches referenced in Microsoft Security Bulletin 07-034 and 07-056.
Windows XP users should also install patch 900930 for Outlook Express.
The Windows Address Book patches are available in 10-096.

Where can I read more about this?

For more information, see Microsoft Security Bulletins 01-038, 02-058, 02-067, 03-003, 04-009, 04-013, 05-030, 06-003, 06-016, 06-043, 06-076, 07-003, 07-034, 07-056, 08-015, and 10-096, US-CERT Alert TA04-070A, and Microsoft Knowledge Base Article 900930.

Technical Details

Service: netbios
wab.exe older than 2010-10-10

Outlook Express vulnerable version, inetcomm.dll dated 2007-2-17

Severity: Area of Concern **CVE:** CVE-2006-2111 CVE-2007-2225 CVE-2007-2227 CVE-2007-3897

Impact

There are several vulnerabilities in e-mail clients, the most severe of which could allow a remote attacker to execute arbitrary commands by sending a specially crafted e-mail message.

Resolution

Install the patches referenced in Microsoft Security Bulletin 01-038 and 08-015 for Outlook. Also, for Outlook 2002, install the patches referenced in 02-067, 03-003, and 04-009, or Office XP service pack 3.

For Outlook Express:
Install the patches referenced in Microsoft Security Bulletin 07-034 and 07-056.
Windows XP users should also install patch 900930 for Outlook Express.
The Windows Address Book patches are available in 10-096.

Where can I read more about this?

For more information, see Microsoft Security Bulletins 01-038, 02-058, 02-067, 03-003, 04-009, 04-013, 05-030, 06-003, 06-016, 06-043, 06-076, 07-003, 07-034, 07-056, 08-015, and 10-096, US-CERT Alert TA04-070A, and Microsoft Knowledge Base Article 900930.

Technical Details

Service: netbios

Inetcomm.dll older than 2007-8-14

Elevation of Privilege Vulnerabilities in Windows Kerberos (MS11-013)

Severity: Area of Concern **CVE:** CVE-2011-0043

Impact

A remote attacker with valid logon credentials could cause a denial of service and elevation of privilege.

Resolution

Apply the fixes referenced in Microsoft Security Bulletins 05-042, 10-014, and 11-013.

Where can I read more about this?

These vulnerabilities were reported in Microsoft Security Bulletins 05-042, 10-014, and 11-013.

Technical Details

Service: netbios
kerberos.dll older than 2010-12-15

Ancillary Function Driver Vulnerability (MS11-046)

Severity: Area of Concern **CVE:** CVE-2011-1249

Impact

The absence of critical updates leads to the potential for denial of service or unauthorized access by attackers or malicious web sites.

The Problems and Resolutions

One or more of the following security updates is not installed on the target system. The resolution is to install the needed updates. This can be done either by following the links in the table, or by visiting the Windows Update service which will automatically determine which updates are needed for your system and help you install them. It is a good idea to make a backup of the system before installing an update, especially for service packs. After the system has been brought up to date, check Microsoft's web site regularly for new critical updates.

Note: The links below apply to the standard editions of Windows operating systems. If you are using a Terminal Server edition, a 64-bit edition, or a non-Intel edition which is not listed, consult the corresponding Microsoft Security Bulletins for patch information.

Update Name	Description	Fix	Bulletin
Ancillary Function Driver	Fixes a vulnerability in the Microsoft Windows Ancillary Function Driver (AFD). A local user with valid login credentials could exploit this vulnerability to elevate privileges by executing a specially crafted application. (CVE 2011-1249)	**XP** 2503665, 2503665 (64-bit) **2003** 2503665, 2503665 (64-bit) **Vista** 2503665, 2503665 (64-bit) **2008** 2503665, 2503665 (64-bit) **Windows 7:**	11-046

	2503665, 2503665 (64-bit) **2008 R2:** 2503665 (64-bit)

Where can I read more about this?

For more information on critical updates, see the Windows critical update pages which are available for Windows 2000, Windows NT 4.0, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7.

Technical Details

Service: netbios
afd.sys older than 2011-2-9

Ancillary Function Driver Vulnerability (MS11-080)

Severity: Area of Concern **CVE:** CVE-2011-2005

Impact

The absence of critical updates leads to the potential for denial of service or unauthorized access by attackers or malicious web sites.

The Problems and Resolutions

One or more of the following security updates is not installed on the target system. The resolution is to install the needed updates. This can be done either by following the links in the table, or by visiting the Windows Update service which will automatically determine which updates are needed for your system and help you install them. It is a good idea to make a backup of the system before installing an update, especially for service packs. After the system has been brought up to date, check Microsoft's web site regularly for new critical updates.

Note: The links below apply to the standard editions of Windows operating systems. If you are using a Terminal Server edition, a 64-bit edition, or a non-Intel edition which is not listed, consult the corresponding Microsoft Security Bulletins for patch information.

Update Name	Description	Fix	Bulletin
Ancillary Function Driver	Fixes a vulnerability in the Microsoft Windows Ancillary Function Driver (AFD). A local user with valid login credentials could exploit this vulnerability to elevate privileges by executing a specially crafted application. (CVE 2011-2005)	**XP** 2592799, 2592799 (64-bit) **2003** 2592799, 2592799 (64-bit)	11-080

Where can I read more about this?

For more information on critical updates, see the Windows critical update pages which are available for Windows 2000, Windows NT 4.0, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7.

Technical Details

Service: netbios
afd.sys older than 2011-8-15

Blended threat privilege elevation vulnerability

Severity: Area of Concern **CVE:** CVE-2008-2540

Impact

The absence of critical updates leads to the potential for denial of service or unauthorized access by attackers or malicious web sites.

The Problems and Resolutions

One or more of the following security updates is not installed on the target system. The resolution is to install the needed updates. This can be done either by following the links in the table, or by visiting the Windows Update service which will automatically determine which updates are needed for your system and help you install them. It is a good idea to make a backup of the system before installing an update, especially for service packs. After the system has been brought up to date, check Microsoft's web site regularly for new critical updates.

Note: The links below apply to the standard editions of Windows operating systems. If you are using a Terminal Server edition, a 64-bit edition, or a non-Intel edition which is not listed, consult the corresponding Microsoft Security Bulletins for patch information.

Update Name	Description	Fix	Bulletin
Blended threat privilege elevation vulnerability	Fixes a privilege elevation vulnerability in Windows 2000, 2003, XP, Vista, and 2008. The vulnerability exists due to a faulty SearchPath function used for locating and opening files on windows. An attacker could exploit the vulnerability by enticing a user to download a crafted file to a specific location and then have them open an application that uses the file. (CVE 2008-2540)	**2000:** 959426 **XP:** 959426 (32 bit), or 959426 (64 bit) **2003:** 959426 (32 bit), 959426 (64 bit), or 959426 Itanium **Vista:** 959426 (32 bit), or 959426 (64 bit) **2008:** 959426 (32 bit), 959426 (64 bit), or 959426 Itanium	09-015

Where can I read more about this?

For more information on critical updates, see the Windows critical update pages which are available for Windows 2000, Windows NT 4.0, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7.

Technical Details

Service: netbios
SOFTWARE\Microsoft\Updates\Windows Server 2003\SP3\KB959426 not found

DirectX MJPEG decompression remote code execution vulnerability

Severity: Area of Concern **CVE:** CVE-2009-0084

Impact

The absence of critical updates leads to the potential for denial of service or unauthorized access by attackers or malicious web sites.

The Problems and Resolutions

One or more of the following security updates is not installed on the target system. The resolution is to install the needed updates. This can be done either by following the links in the table, or by visiting the Windows Update service which will automatically determine which updates are needed for your system and help you install them. It is a good idea to make a backup of the system before installing an update, especially for service packs. After the system has been brought up to date, check Microsoft's web site regularly for new critical updates.

Note: The links below apply to the standard editions of Windows operating systems. If you are using a Terminal Server edition, a 64-bit edition, or a non-Intel edition which is not listed, consult the corresponding Microsoft Security Bulletins for patch information.

Update Name	Description	Fix	Bulletin
DirectX MJPEG decompression remote code execution	Corrects the way the DirectShow component of DirectX decompresses media files. CVE 2009-0084)	**2000 (8.1):** 961373 **2000 (9.0->9.0c):** 961373 **XP:** 32-bit: 961373 64-bit: 96173 **2003:** 32-bit: 961373 64-bit: 961373 Itanium: 961373	09-011

Where can I read more about this?

For more information on critical updates, see the Windows critical update pages which are available for Windows 2000, Windows NT 4.0, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7.

Technical Details

Service: netbios
SOFTWARE\Microsoft\Updates\Windows Server 2003\SP3\KB961373 not found

DirectX SAMI-MJPEG parsing remote code execution for DirectX 9.0c

Severity: Area of Concern **CVE:** CVE-2008-0011

Impact

The absence of critical updates leads to the potential for denial of service or unauthorized access by attackers or malicious web sites.

The Problems and Resolutions

One or more of the following security updates is not installed on the target system. The resolution is to install the needed updates. This can be done either by following the links in the table, or by visiting the Windows Update service which will automatically determine which updates are needed for your system and help you install them. It is a good idea to make a backup of the system before installing an update, especially for service packs. After the system has been brought up to date, check Microsoft's web site regularly for new critical updates.

Note: The links below apply to the standard editions of Windows operating systems. If you are using a Terminal Server edition, a 64-bit edition, or a non-Intel edition which is not listed, consult the corresponding Microsoft Security Bulletins for patch information.

Update Name	Description	Fix	Bulletin
DirectX SAMI-MJPEG Parsing Remote Code Execution	Fixed vulnerabilities that could allow remote code execution parsing MJPEG and SAMI files. (CVE 2008-0011 CVE 2008-1444)	**2000:** 951698 **XP:** 951698 **2003:** 951698 **Vista:** 951698 **2008:** 951698	08-033

Where can I read more about this?

For more information on critical updates, see the Windows critical update pages which are available for Windows 2000, Windows NT 4.0, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7.

Technical Details

Service: netbios
SOFTWARE\Microsoft\Updates\Windows Server 2003\SP3\KB951698 not found

DirectX parsing remote code execution for DirectX 9.0c

Severity: Area of Concern **CVE:** CVE-2007-3895

Impact

The absence of critical updates leads to the potential for denial of service or unauthorized access by attackers or malicious web sites.

The Problems and Resolutions

One or more of the following security updates is not installed on the target system. The resolution is to install the needed updates. This can be done either by following the links in the table, or by visiting the Windows Update service which will automatically determine which updates are needed for your system and help you install them. It is a good idea to make a backup of the system before installing an update, especially for service packs. After the system has been brought up to date, check Microsoft's web site regularly for new critical updates.

Note: The links below apply to the standard editions of Windows operating systems. If you are using a Terminal Server edition, a 64-bit edition, or a non-Intel edition which is not listed, consult the corresponding Microsoft Security Bulletins for patch information.

Update Name	Description	Fix	Bulletin
DirectX Parsing Remote Code Execution	Fixed vulnerabilities that could allow remote code execution parsing SAMI, WAV or AVI files. (CVE 2007-3895 CVE 2007-3901)	**2000 (7.0):** 941568 **2000 (8.0):** 941568 **2000 (9.0c):** 941568 **XP:** 941568 **2003:** 941568 **Vista:** 941568	07-064

Where can I read more about this?

For more information on critical updates, see the Windows critical update pages which are available for Windows 2000, Windows NT 4.0, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7.

Technical Details

Service: netbios
SOFTWARE\Microsoft\Updates\Windows Server 2003\SP3\KB941568 not found

Elevation of Privilege Vulnerabilities in Windows (MS09-012)

Severity: Area of Concern **CVE:** CVE-2008-1436 CVE-2009-0078 CVE-2009-0079

Impact

The absence of critical updates leads to the potential for denial of service or unauthorized access by attackers or malicious web sites.

The Problems and Resolutions

One or more of the following security updates is not installed on the target system. The resolution is to install the needed updates. This can be done either by following the links in the table, or by visiting the Windows Update service which will automatically determine which updates are needed for your system and help you install them. It is a good idea to make a backup of the system before installing an update, especially for service packs. After the system has been brought up to date, check Microsoft's web site regularly for new critical updates.

Note: The links below apply to the standard editions of Windows operating systems. If you are using a Terminal Server edition, a 64-bit edition, or a non-Intel edition which is not listed, consult the corresponding Microsoft Security Bulletins for patch information.

Update Name	Description	Fix	Bulletin
Elevation of Privilege Vulnerabilities in Windows	Fixes multiple privilege elevation vulnerabilities. (CVE 2008-4036 CVE 2008-1436 CVE 2009-0078 CVE 2009-0079 CVE 2009-0080)	**2000:** 952004 **XP:** 952004 **2003:** 952004 **Vista:** 952004 **2008:** 952004	08-064 09-012

Where can I read more about this?

For more information on critical updates, see the Windows critical update pages which are available for Windows 2000, Windows NT 4.0, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7.

Technical Details

Service: netbios
msdtcprx.dll older than 2008-7-23

Elevation of Privilege Vulnerabilities in Windows (MS10-015)

Severity: Area of Concern **CVE:** CVE-2010-0232 CVE-2010-0233

Impact

The absence of critical updates leads to the potential for denial of service or unauthorized access by attackers or malicious web sites.

The Problems and Resolutions

One or more of the following security updates is not installed on the target system. The resolution is to install the needed updates. This can be done either by following the links in the table, or by visiting the Windows Update service which will automatically determine which updates are needed for your system and help you install them. It is a good idea to make a backup of the system before installing an update, especially for service packs. After the system has been brought up to date, check Microsoft's web site regularly for new critical updates.

Note: The links below apply to the standard editions of Windows operating systems. If you are using a Terminal Server edition, a 64-bit edition, or a non-Intel edition which is not listed, consult the corresponding Microsoft Security Bulletins for patch information.

Update Name	Description	Fix	Bulletin
Windows kernel vulnerable version	Fixes multiple vulnerabilities which allow authenticated users to elevate privileges on Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7. (CVE 2009-2515 CVE 2009-2516 CVE 2009-2517 CVE 2010-0232 CVE 2010-0233)	**2000:** 977165 **XP:** 977165 **2003:** 977165 **Vista:** 977165 **2008:** 977165 **Windows 7:** 977165	09-058 10-015

Where can I read more about this?

For more information on critical updates, see the Windows critical update pages which are available for Windows 2000, Windows NT 4.0, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7.

Technical Details

Service: netbios
ntoskrnl.exe older than 2009-12-14

Elevation of Privilege Vulnerabilities in Windows (MS11-062)

Severity: Area of Concern **CVE:** CVE-2011-1974

Impact

The absence of critical updates leads to the potential for denial of service or unauthorized access by attackers or malicious web sites.

The Problems and Resolutions

One or more of the following security updates is not installed on the target system. The resolution is to install the needed updates. This can be done either by following the links in the table, or by visiting the Windows Update service which will automatically determine which updates are needed for your system and help you install them. It is a good idea to make a backup of the system before installing an update, especially for service packs. After the system has been brought up to date, check Microsoft's web site regularly for new critical updates.

Note: The links below apply to the standard editions of Windows operating systems. If you are using a Terminal Server edition, a 64-bit edition, or a non-Intel edition which is not listed, consult the corresponding Microsoft Security Bulletins for patch information.

Update Name	Description	Fix	Bulletin
Elevation of Privilege Vulnerabilities in Windows (MS11-062)	Fixes a vulnerability in Remote Access Service NDISTAPI driver. (CVE 2011-1974)	**XP** 2566454, 2566454 (64-bit) **2003** 2566454, 2566454 (64-bit)	11-062

Where can I read more about this?

For more information on critical updates, see the Windows critical update pages which are available for Windows 2000, Windows NT 4.0, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7.

Technical Details

Service: netbios
ndistapi.sys older than 2011-7-6

Insecure Library Loading in Internet Connection Signup Wizard Could Allow Remote Code

Severity: Area of Concern **CVE:** CVE-2010-3144

Impact

The absence of critical updates leads to the potential for denial of service or unauthorized access by attackers or malicious web sites.

The Problems and Resolutions

One or more of the following security updates is not installed on the target system. The resolution is to install the needed updates. This can be done either by following the links in the table, or by visiting the Windows Update service which will automatically determine which updates are needed for your system and help you install them. It is a good idea to make a backup of the system before installing an update, especially for

service packs. After the system has been brought up to date, check Microsoft's web site regularly for new critical updates.

Note: The links below apply to the standard editions of Windows operating systems. If you are using a Terminal Server edition, a 64-bit edition, or a non-Intel edition which is not listed, consult the corresponding Microsoft Security Bulletins for patch information.

Update Name	Description	Fix	Bulletin
Insecure Library Loading in Internet Connection Signup Wizard Could Allow Remote Code Execution	Fixes a vulnerability that could allow remote code execution if a user opens an `.ins` or `.isp` file located in the same network folder as a specially crafted library file. For an attack to be successful, a user must visit an untrusted remote file system location or WebDAV share and open a document from this location that is then loaded by a vulnerable application. (CVE 2010-3144)	**XP:** KB2443105 **2003:** KB2443105	10-097

Where can I read more about this?

For more information on critical updates, see the Windows critical update pages which are available for Windows 2000, Windows NT 4.0, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7.

Technical Details

Service: netbios
isign32.dll older than 2010-11-18

Kernel-Mode Drivers vulnerabilities

Severity: Area of Concern **CVE:** CVE-2011-0086 CVE-2011-0087 CVE-2011-0088 CVE-2011-0089 CVE-2011-0090

Impact

The absence of critical updates leads to the potential for denial of service or unauthorized access by attackers or malicious web sites.

The Problems and Resolutions

One or more of the following security updates is not installed on the target system. The resolution is to install the needed updates. This can be done either by following the links in the table, or by visiting the Windows Update service which will automatically determine which updates are needed for your system and help you install them. It is a good idea to make a backup of the system before installing an update, especially for service packs. After the system has been brought up to date, check Microsoft's web site regularly for new critical updates.

Note: The links below apply to the standard editions of Windows operating systems. If you are using a Terminal Server edition, a 64-bit edition, or a non-Intel edition which is not listed, consult the corresponding

Microsoft Security Bulletins for patch information.

Update Name	Description	Fix	Bulletin
Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege	Fixes vulnerabilities which could allow elevation of privilege if an attacker logged on locally and ran a specially crafted application. An attacker must have valid logon credentials and be able to log on locally to exploit these vulnerabilities. (CVE 2011-0662 CVE 2011-0665 CVE 2011-0666 CVE 2011-0667 CVE 2011-0670 CVE 2011-0671 CVE 2011-0672 CVE 2011-0673 CVE 2011-0674 CVE 2011-0675 CVE 2011-0676 CVE 2011-0677 CVE 2011-1225 CVE 2011-1226 CVE 2011-1227 CVE 2011-1228 CVE 2011-1229 CVE 2011-1230 CVE 2011-1231 CVE 2011-1232 CVE 2011-1233 CVE 2011-1234 CVE 2011-1235 CVE 2011-1236 CVE 2011-1237 CVE 2011-1238 CVE 2011-1239 CVE 2011-1240 CVE 2011-1241 CVE 2011-1242) Also fixes five vulnerabilities which could allow elevation of privileges if an attacker logged on locally and was able to execute a specially crafted program. (CVE 2011-0086 CVE 2011-0087 CVE 2011-0088 CVE 2011-0089 CVE 2011-0090)	**XP:** KB2506223 **2003:** KB2506223 **Vista:** KB2506223 **2008:** KB2506223 **Windows 7:** KB2506223	11-034 11-012

Where can I read more about this?

For more information on critical updates, see the Windows critical update pages which are available for Windows 2000, Windows NT 4.0, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7.

Technical Details

Service: netbios
win32k.sys older than 2010-12-30

MHTML Mime-formatted information disclosure

Severity: Area of Concern **CVE:** CVE-2011-1894

Impact

The absence of critical updates leads to the potential for denial of service or unauthorized access by attackers or malicious web sites.

The Problems and Resolutions

Impact

Intrusion attempts or other unauthorized activities could go unnoticed.

Resolution

Edit the auditing policy, which is found in the *Local Security Policy* under *Administrative Tools* on most systems.

Note that if there is an *Effective Setting* in the local security policy, it is this setting which is used. This setting can only be changed on the domain controller.

Where can I read more about this?

See Microsoft's guide to setting up auditing and developing an auditing policy.

Technical Details

Service: netbios-ssn

object access auditing disabled

Severity: Potential Problem **CVE:** CVE-1999-0575

Impact

Intrusion attempts or other unauthorized activities could go unnoticed.

Resolution

Edit the auditing policy, which is found in the *Local Security Policy* under *Administrative Tools* on most systems.

Note that if there is an *Effective Setting* in the local security policy, it is this setting which is used. This setting can only be changed on the domain controller.

Where can I read more about this?

See Microsoft's guide to setting up auditing and developing an auditing policy.

Technical Details

Service: netbios-ssn

object access failure auditing disabled

Severity: Potential Problem **CVE:** CVE-1999-0575

Impact

Intrusion attempts or other unauthorized activities could go unnoticed.

Resolution

Edit the auditing policy, which is found in the *Local Security Policy* under *Administrative Tools* on most systems.

Note that if there is an *Effective Setting* in the local security policy, it is this setting which is used. This setting can only be changed on the domain controller.

Where can I read more about this?

See Microsoft's guide to setting up auditing and developing an auditing policy.

Technical Details

Service: netbios-ssn

policy change auditing disabled

Severity: Potential Problem **CVE:** CVE-1999-0575

Impact

Intrusion attempts or other unauthorized activities could go unnoticed.

Resolution

Edit the auditing policy, which is found in the *Local Security Policy* under *Administrative Tools* on most systems.

Note that if there is an *Effective Setting* in the local security policy, it is this setting which is used. This setting can only be changed on the domain controller.

Where can I read more about this?

See Microsoft's guide to setting up auditing and developing an auditing policy.

Technical Details

Service: netbios-ssn

policy change failure auditing disabled

Severity: Potential Problem **CVE:** CVE-1999-0575

Impact

Intrusion attempts or other unauthorized activities could go unnoticed.

Resolution

Edit the auditing policy, which is found in the *Local Security Policy* under *Administrative Tools* on most systems.

Note that if there is an *Effective Setting* in the local security policy, it is this setting which is used. This setting can only be changed on the domain controller.

Where can I read more about this?

See Microsoft's guide to setting up auditing and developing an auditing policy.

Technical Details

Service: netbios-ssn

system event auditing disabled

Severity: Potential Problem **CVE:** CVE-1999-0575

Impact

Intrusion attempts or other unauthorized activities could go unnoticed.

Resolution

Edit the auditing policy, which is found in the *Local Security Policy* under *Administrative Tools* on most systems.

Note that if there is an *Effective Setting* in the local security policy, it is this setting which is used. This setting can only be changed on the domain controller.

Where can I read more about this?

See Microsoft's guide to setting up auditing and developing an auditing policy.

Technical Details

Service: netbios-ssn

system event failure auditing disabled

Severity: Potential Problem **CVE:** CVE-1999-0575

Impact

Intrusion attempts or other unauthorized activities could go unnoticed.

Resolution

Edit the auditing policy, which is found in the *Local Security Policy* under *Administrative Tools* on most systems.

Note that if there is an *Effective Setting* in the local security policy, it is this setting which is used. This setting can only be changed on the domain controller.

Where can I read more about this?

See Microsoft's guide to setting up auditing and developing an auditing policy.

Technical Details

Service: netbios-ssn

Windows administrator account not renamed

Severity: Potential Problem **CVE:** CVE-1999-0585

Impact

The default administrator and guest account names give attackers a starting point for conducting brute-force password guessing attacks.

Resolution

Change the name of the administrator and guest accounts. To do this on Active Directory servers, open *Active Directory Users and Computers*. Click *Users*, then right-click on Administrator or Guest, and select *Rename*. To do this on workstations, open the *Local Security Policy* from the Administrative Tools menu. Choose *Local Policies*, then *Security Options*, then Accounts: Rename administrator or guest account.

Where can I read more about this?

For more information on securing the administrator account, see The Administrator Accounts Security Planning Guide - Chapter 3.

Technical Details

Service: netbios-ssn
UID 500 = Administrator

Windows guest account not renamed

Severity: Potential Problem

Impact

The default administrator and guest account names give attackers a starting point for conducting brute-force password guessing attacks.

Resolution

Change the name of the administrator and guest accounts. To do this on Active Directory servers, open *Active Directory Users and Computers*. Click *Users*, then right-click on Administrator or Guest, and select *Rename*. To do this on workstations, open the *Local Security Policy* from the Administrative Tools menu. Choose *Local Policies*, then *Security Options*, then Accounts: Rename administrator or guest account.

Where can I read more about this?

For more information on securing the administrator account, see The Administrator Accounts Security Planning Guide - Chapter 3.

Technical Details

Service: netbios-ssn
UID 501 = Guest

Password never expires for user localuser

Severity: Potential Problem

Impact

If a password becomes compromised, it can be used to gain unauthorized access for an unlimited period of time.

Resolution

Enable password expiration for all users. This is done by removing the check mark beside *password never expires* in the user's properties.

Where can I read more about this?

More information on best practices related to password security is available from Microsoft.

Technical Details

Service: netbios-ssn
Password never expires for user localuser

Windows TCP/IP Stack not hardened

Severity: Potential Problem

Impact

A remote attacker could cause a temporary denial of service.

Resolution

Apply the TCP/IP stack hardening guidelines discussed in Microsoft Knowledge Base Article 324270 for Windows Server 2003 or 315669 for Windows XP. (Although the latter article was written for Windows 2000, it is presumably also effective for Windows XP.) The patch referenced in Microsoft Security Bulletin 05-019 also fixes this vulnerability, but not for IPv6 interfaces.

Where can I read more about this?

Land was originally reported in CERT Advisory 1997-28. The Land attack relating to Windows XP Service Pack 2 and Windows Server 2003 was posted to Bugtraq. The Land attack relating to IPv6 was posted to NTBugtraq.

Technical Details

Service: netbios
KB324270/315669 recommendations not applied for XP SP2 or 2003

Microsoft Windows Insecure Library Loading vulnerability

Severity: Potential Problem

Impact

The absence of critical updates leads to the potential for denial of service or unauthorized access by attackers

or malicious web sites.

The Problems and Resolutions

One or more of the following security updates is not installed on the target system. The resolution is to install the needed updates. This can be done either by following the links in the table, or by visiting the Windows Update service which will automatically determine which updates are needed for your system and help you install them. It is a good idea to make a backup of the system before installing an update, especially for service packs. After the system has been brought up to date, check Microsoft's web site regularly for new critical updates.

Note: The links below apply to the standard editions of Windows operating systems. If you are using a Terminal Server edition, a 64-bit edition, or a non-Intel edition which is not listed, consult the corresponding Microsoft Security Bulletins for patch information.

Update Name	Description	Fix	Bulletin
Microsoft Windows Insecure Library Loading vulnerability	A remote attacker could execute DLL preloading attacks through an SMB share or WebDAV.	Disable loading of libraries from WebDAV and remote network shares as described in Microsoft KB 2264107.	2269637

Where can I read more about this?

For more information on critical updates, see the Windows critical update pages which are available for Windows 2000, Windows NT 4.0, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7.

Technical Details

Service: netbios
SYSTEM\CurrentControlSet\Control\Session Manager\CWDIllegalInDllSearch does not exist

Microsoft Windows Service Isolation Bypass Local Privilege Escalation

Severity: Potential Problem **CVE:** CVE-2010-1886

Impact

The absence of critical updates leads to the potential for denial of service or unauthorized access by attackers or malicious web sites.

The Problems and Resolutions

One or more of the following security updates is not installed on the target system. The resolution is to install the needed updates. This can be done either by following the links in the table, or by visiting the Windows Update service which will automatically determine which updates are needed for your system and help you install them. It is a good idea to make a backup of the system before installing an update, especially for service packs. After the system has been brought up to date, check Microsoft's web site regularly for new critical updates.

Note: The links below apply to the standard editions of Windows operating systems. If you are using a Terminal Server edition, a 64-bit edition, or a non-Intel edition which is not listed, consult the corresponding Microsoft Security Bulletins for patch information.

Update Name	Description	Fix	Bulletin
Microsoft Windows Service Isolation Bypass Local Privilege Escalation	Fixed a vulnerability which leverages the Windows Service Isolation feature to gain elevation of privilege. (CVE 2010-1886)	**TAPI** 982316	2264072

Where can I read more about this?

For more information on critical updates, see the Windows critical update pages which are available for Windows 2000, Windows NT 4.0, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7.

Technical Details

Service: netbios
Tapisrv.dll older than 2010-4-22

Multiple Windows TCP/IP vulnerabilities (MS08-001)

Severity: Potential Problem **CVE:** CVE-2007-0066 CVE-2007-0069

Impact

The absence of critical updates leads to the potential for denial of service or unauthorized access by attackers or malicious web sites.

The Problems and Resolutions

One or more of the following security updates is not installed on the target system. The resolution is to install the needed updates. This can be done either by following the links in the table, or by visiting the Windows Update service which will automatically determine which updates are needed for your system and help you install them. It is a good idea to make a backup of the system before installing an update, especially for service packs. After the system has been brought up to date, check Microsoft's web site regularly for new critical updates.

Note: The links below apply to the standard editions of Windows operating systems. If you are using a Terminal Server edition, a 64-bit edition, or a non-Intel edition which is not listed, consult the corresponding Microsoft Security Bulletins for patch information.

Update Name	Description	Fix	Bulletin
Multiple Windows TCP/IP vulnerabilities	Fixes two vulnerabilities: (1) an IGMPv3 and MLDv2 vulnerability that could allow remote code execution; and (2) an ICMP vulnerability that could result in denial of service. (CVE 2007-0069, CVE 2007-0066)	**2000:** 941644 **XP:** 941644 **2003:** 941644 **Vista:** 941644	08-001

Where can I read more about this?

For more information on critical updates, see the Windows critical update pages which are available for Windows 2000, Windows NT 4.0, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7.

Technical Details

Service: netbios
tcpip.sys older than 2007-10-29

Windows Embedded OpenType Font Engine Vulnerability

Severity: Potential Problem **CVE:** CVE-2010-0018

Impact

The absence of critical updates leads to the potential for denial of service or unauthorized access by attackers or malicious web sites.

The Problems and Resolutions

One or more of the following security updates is not installed on the target system. The resolution is to install the needed updates. This can be done either by following the links in the table, or by visiting the Windows Update service which will automatically determine which updates are needed for your system and help you install them. It is a good idea to make a backup of the system before installing an update, especially for service packs. After the system has been brought up to date, check Microsoft's web site regularly for new critical updates.

Note: The links below apply to the standard editions of Windows operating systems. If you are using a Terminal Server edition, a 64-bit edition, or a non-Intel edition which is not listed, consult the corresponding Microsoft Security Bulletins for patch information.

Update Name	Description	Fix	Bulletin
Windows Embedded OpenType Font Engine Vulnerability	Fixes a remote code execution vulnerability in Windows 2000, 2003, XP, Vista, 7, and Server 2008. The vulnerability exists due to the way Windows Embedded OpenType (EOT) Font Engine decompresses specially crafted EOT fonts. (CVE 2010-0018)	**2000:** 972270 **2003:** 972270 (32-bit), 972270 (64-bit) **XP:** 972270 (32-bit), 972270 (64-bit) **Vista:** 972270 (32-bit), 972270 (64-bit) **Windows 7:** 972270 **2008:** 972270 (32-bit), 972270 (64-bit)	10-001

Where can I read more about this?

For more information on critical updates, see the Windows critical update pages which are available for Windows 2000, Windows NT 4.0, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7.

Technical Details

Service: netbios
fontsub.dll older than 2009-10-14

1025/UDP

Severity: Service

Technical Details

1038/TCP

Severity: Service

Technical Details

1718/UDP

Severity: Service

Technical Details

1719/UDP

Severity: Service

Technical Details

DNS

Severity: Service

Technical Details

SMB

Severity: Service

Technical Details

\131\000\000\001\143

XDM (X login)

Severity: Service

Technical Details

epmap (135/TCP)

Severity: Service

Technical Details

isakmp (500/UDP)

Severity: Service

Technical Details

microsoft-ds (445/TCP)

Severity: Service

Technical Details

microsoft-ds (445/UDP)

Severity: Service

Technical Details

netbios-dgm (138/UDP)

Severity: Service

Technical Details

netbios-ns (137/UDP)

Severity: Service

Technical Details

ntp (123/UDP)

Severity: Service

Technical Details

tftp (69/UDP)

Severity: Service

Technical Details

Scan Session: saint-data_nerc; Scan Policy: NERC CIP; Scan Data Set: 1 November 2011 11:44