The Vulnerabilities In Windows XP

# CVE ID CWE ID # of Exploits Vulnerability Type(s) Publish Date Update Date Score Gained Access Level Access Complexity Authentication Conf. Integ. Avail.

1 CVE-2011-5046 20 1 DoS Exec Code Mem. Corr. 2011-12-30 2018-10-12 9.3 None Remote Medium Not required Complete Complete Complete

The Graphics Device Interface (GDI) in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 (service pack version) and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly validate user-mode input, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted data, as demonstrated by a large height attribute of an IFRAME element rendered by Safari, aka "GDI Access Violation Vulnerability."

2 CVE-2011-3417 264 2011-12-30 2020-09-28 9.3 None Remote Medium Not required Complete Complete Complete

The Forms Authentication feature in the ASP.NET subsystem in Microsoft .NET Framework 1.1 SP1, 2.0 SP2, 3.5 SP1, 3.5.1, and 4.0, when sliding expiry is enabled, does not properly handle cached content, which allows remote attackers to obtain access to arbitrary user accounts via a crafted URL, aka "ASP.NET Forms Authentication Ticket Caching Vulnerability."

3 CVE-2011-3416 264 Bypass 2011-12-30 2020-09-28 8.5 None Remote Medium ??? Complete Complete Complete

The Forms Authentication feature in the ASP.NET subsystem in Microsoft .NET Framework 1.1 SP1, 2.0 SP2, 3.5 SP1, 3.5.1, and 4.0 allows remote authenticated users to obtain access to arbitrary user accounts via a crafted username, aka "ASP.Net Forms Authentication Bypass

Vulnerability."

4 CVE-2011-3415 20 2011-12-30 2020-09-28 6.8 None Remote Medium Not required Partial Partial Partial

Open redirect vulnerability in the Forms Authentication feature in the ASP.NET subsystem in Microsoft .NET Framework 2.0 SP2, 3.5 SP1, 3.5.1, and 4.0 allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via a crafted return URL, aka "Insecure Redirect in .NET Form Authentication Vulnerability."

5 CVE-2011-3414 399 DoS 2011-12-30 2020-09-28 7.8 None Remote Low Not required None None Complete

The CaseInsensitiveHashProvider.getHashCode function in the HashTable implementation in the ASP.NET subsystem in Microsoft .NET Framework 1.1 SP1, 2.0 SP2, 3.5 SP1, 3.5.1, and 4.0 computes hash values for form parameters without restricting the ability to trigger hash collisions predictably, which allows remote attackers to cause a denial of service (CPU consumption) by sending many crafted parameters, aka "Collisions in HashTable May Cause DoS Vulnerability."

6 CVE-2011-3408 264 +Priv 2011-12-14 2020-09-28 7.2 None Local Low Not required Complete Complete Complete

Csrsrv.dll in the Client/Server Run-time Subsystem (aka CSRSS) in the Win32 subsystem in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly check permissions for sending inter-process device-event messages from low-integrity processes to high-integrity processes, which allows local users to gain privileges via a crafted application, aka "CSRSS Local Privilege Elevation Vulnerability."

7 CVE-2011-3406 119 Exec Code Overflow 2011-12-14 2020-09-28 9.0 None Remote Low ??? Complete Complete Complete

Buffer overflow in Active Directory, Active Directory Application Mode (ADAM), and Active Directory Lightweight Directory Service (AD LDS) in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote authenticated users to execute arbitrary code via a crafted query that leverages incorrect memory initialization, aka "Active Directory Buffer Overflow Vulnerability."

8 CVE-2011-3402 Exec Code 2011-11-04 2020-09-28 9.3 None Remote Medium Not required Complete Complete Complete

Unspecified vulnerability in the TrueType font parsing engine in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote attackers to execute arbitrary code via crafted font data in a Word document or web page, as exploited in the wild in November 2011 by Duqu, aka "TrueType Font Parsing Vulnerability."

9 CVE-2011-3401 94 Exec Code Mem. Corr. 2011-12-14 2018-10-30 9.3 None Remote Medium Not required Complete Complete Complete

ENCDEC.DLL in Windows Media Player and Media Center in Microsoft Windows XP SP2 and SP3, Windows Vista SP2, and Windows 7 Gold and SP1 allows remote attackers to execute arbitrary code via a crafted .dvr-ms file, aka "Windows Media Player DVR-MS Memory Corruption Vulnerability."

10 CVE-2011-3400 94 Exec Code 2011-12-14 2019-02-26 9.3 None Remote Medium Not required Complete Complete Complete

Microsoft Windows XP SP2 and SP3 and Server 2003 SP2 do not properly handle OLE objects in memory, which allows remote attackers to execute arbitrary code via a crafted object in a file, aka "OLE Property Vulnerability."

11 CVE-2011-3397 94 Exec Code 2011-12-14 2019-02-26 9.3 None Remote Medium Not required Complete Complete Complete

The Microsoft Time component in DATIME.DLL in Microsoft Windows XP SP2 and SP3 and Server 2003 SP2 allows remote attackers to execute arbitrary code via a crafted web site that leverages an unspecified "binary behavior" in Internet Explorer, aka "Microsoft Time Remote Code Execution Vulnerability."

12 CVE-2011-2600 264 DoS 2011-06-30 2011-07-12 7.1 None Remote Medium Not required None None Complete

The GPU support functionality in Windows XP does not properly restrict rendering time, which allows remote attackers to cause a denial of service (system crash) via vectors involving WebGL and (1) shader programs or (2) complex 3D geometry, as demonstrated by using Mozilla Firefox or Google Chrome to visit the lots-of-polys-example.html test page in the Khronos WebGL SDK.

13 CVE-2011-2018 264 +Priv 2011-12-14 2018-10-30 7.2 None Local Low Not required Complete Complete Complete

The kernel in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, and Windows 7 Gold and SP1 does not properly initialize objects, which allows local users to gain privileges via a crafted application, aka "Windows Kernel Exception Handler Vulnerability."

14 CVE-2011-2014 287 Bypass 2011-11-08 2020-09-28 9.0 None Remote Low ??? Complete Complete Complete

The LDAP over SSL (aka LDAPS) implementation in Active Directory, Active Directory Application Mode (ADAM), and Active Directory Lightweight Directory Service (AD LDS) in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not examine Certificate Revocation Lists (CRLs), which allows remote authenticated users to bypass intended certificate restrictions and access Active Directory resources by leveraging a revoked X.509 certificate for a domain account, aka "LDAPS Authentication Bypass Vulnerability."

15 CVE-2011-2011 399 +Priv 2011-10-12 2020-09-28 7.2 None Local Low Not required Complete Complete Complete

Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, aka "Win32k Use After Free Vulnerability."

16 CVE-2011-2005 264 +Priv 2011-10-12 2019-02-26 7.2 None Local Low Not required Complete Complete Complete

afd.sys in the Ancillary Function Driver in Microsoft Windows XP SP2 and SP3 and Server 2003 SP2 does not properly validate user-mode input passed to kernel mode, which allows local users to gain privileges via a crafted application, aka "Ancillary Function Driver Elevation of Privilege Vulnerability."

17 CVE-2011-2003 119 Exec Code Overflow 2011-10-12 2020-09-28 9.3 None Remote Medium Not required Complete Complete Complete

Buffer overflow in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote attackers to execute arbitrary code via a crafted .fon file, aka "Font Library File Buffer Overrun Vulnerability."

18 CVE-2011-1991 +Priv 2011-09-15 2020-09-28 9.3 None Remote Medium Not required Complete Complete Complete

Multiple untrusted search path vulnerabilities in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allow local users to gain privileges via a Trojan horse DLL in the current working directory, as demonstrated by a directory that contains a .doc, .rtf, or .txt file, related to (1) deskpan.dll in the Display Panning CPL Extension, (2) EAPHost Authenticator Service, (3) Folder Redirection, (4) HyperTerminal, (5) the Japanese Input Method Editor (IME), and (6) Microsoft Management Console (MMC), aka "Windows Components Insecure Library Loading Vulnerability."

19 CVE-2011-1985 DoS +Priv 2011-10-12 2020-09-28 7.2 None Local Low Not required Complete Complete Complete

win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly validate user-mode input, which allows local users to gain privileges or cause a denial of service (NULL pointer dereference and system crash) via a crafted application, aka "Win32k Null Pointer De-reference Vulnerability."

20 CVE-2011-1974 264 +Priv 2011-08-10 2019-02-26 7.2 None Local Low Not required Complete Complete Complete

NDISTAPI.sys in the NDISTAPI driver in Remote Access Service (RAS) in Microsoft Windows XP SP2 and SP3 and Windows Server 2003 SP2 does not properly validate user-mode input, which allows local users to gain privileges via a crafted application, aka "NDISTAPI Elevation of Privilege Vulnerability."

21 CVE-2011-1968 399 DoS 2011-08-10 2019-02-26 7.1 None Remote Medium Not required None None Complete

The Remote Desktop Protocol (RDP) implementation in Microsoft Windows XP SP2 and SP3 and Windows Server 2003 SP2 does not properly process packets in memory, which allows remote attackers to cause a denial of service (reboot) by sending crafted RDP packets triggering access to an object that (1) was not properly initialized or (2) is deleted, as exploited in the wild in 2011, aka "Remote Desktop Protocol Vulnerability."

22 CVE-2011-1967 264 +Priv 2011-08-10 2020-09-28 7.2 None Local Low Not required Complete Complete Complete

Winsrv.dll in the Client/Server Run-time Subsystem (aka CSRSS) in the Win32 subsystem in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly check permissions for sending inter-process device-event messages from low-integrity processes to high-integrity processes, which allows local users to gain privileges via a crafted application, aka "CSRSS Vulnerability."

23 CVE-2011-1894 79 XSS 2011-06-16 2019-02-26 4.3 None Remote Medium Not required None Partial None

The MHTML protocol handler in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly handle a MIME format in a request for embedded content in an HTML document, which allows remote attackers to conduct cross-site scripting (XSS) attacks via a crafted EMBED element in a web page that is visited in Internet Explorer, aka "MHTML Mime-Formatted Request Vulnerability."

24 CVE-2011-1886 2011-07-13 2018-10-12 2.1 None Local Low Not required Partial None None

win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP3 does not properly validate the arguments to functions, which allows local users to read arbitrary data from kernel memory via a crafted application that triggers a NULL pointer dereference, aka "Win32k Incorrect Parameter Validation Allows Information Disclosure Vulnerability."

25 CVE-2011-1885 +Priv 2011-07-13 2020-09-28 7.2 None Local Low Not required Complete Complete Complete

win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that triggers a NULL pointer dereference, a different vulnerability than other CVEs listed in MS11-054, aka "Win32k Null Pointer De-reference Vulnerability."

26 CVE-2011-1884 399 +Priv 2011-07-13 2020-09-28 7.2 None Local Low Not required Complete Complete Complete

Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other CVEs listed in MS11-054, aka "Win32k Use After Free Vulnerability."

27 CVE-2011-1883 399 +Priv 2011-07-13 2020-09-28 7.2 None Local Low Not required Complete Complete Complete

Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other CVEs listed in MS11-054, aka "Win32k Use After Free Vulnerability."

28 CVE-2011-1882 399 +Priv 2011-07-13 2020-09-28 7.2 None Local Low Not required Complete Complete Complete

Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other CVEs listed in MS11-054, aka "Win32k Use After Free Vulnerability."

29 CVE-2011-1881 +Priv 2011-07-13 2020-09-28 7.2 None Local Low Not required Complete Complete Complete

win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that triggers a NULL pointer dereference, a different vulnerability than other CVEs listed in MS11-054, aka "Win32k Null Pointer De-reference Vulnerability."

30 CVE-2011-1880 +Priv 2011-07-13 2020-09-28 7.2 None Local Low Not required Complete Complete Complete

win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that triggers a NULL pointer dereference, a different vulnerability than other CVEs listed in MS11-054, aka "Win32k Null Pointer De-reference Vulnerability."

31 CVE-2011-1879 399 +Priv 2011-07-13 2020-09-28 7.2 None Local Low Not required Complete Complete Complete

Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other CVEs listed in MS11-054, aka "Win32k Use After Free Vulnerability."

32 CVE-2011-1878 399 +Priv 2011-07-13 2020-09-28 7.2 None Local Low Not required Complete Complete Complete

Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other CVEs listed in MS11-054, aka "Win32k Use After Free Vulnerability."

33 CVE-2011-1876 399 +Priv 2011-07-13 2020-09-28 7.2 None Local Low Not required Complete Complete Complete

Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other CVEs listed in MS11-054, aka "Win32k Use After Free Vulnerability."

34 CVE-2011-1875 399 +Priv 2011-07-13 2020-09-28 7.2 None Local Low Not required Complete Complete Complete

Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other CVEs listed in MS11-054, aka "Win32k Use After Free Vulnerability."

35 CVE-2011-1874 399 +Priv 2011-07-13 2020-09-28 7.2 None Local Low Not required Complete Complete Complete

Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other CVEs listed in MS11-054, aka "Win32k Use After Free Vulnerability."

36 CVE-2011-1873 20 Exec Code 2011-06-16 2020-09-28 9.3 None Remote Medium Not required Complete Complete Complete

win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 on 64-bit platforms does not properly validate pointers during the parsing of OpenType (aka OTF) fonts, which allows remote attackers to execute arbitrary code via a crafted font file, aka "Win32k OTF Validation Vulnerability."

37 CVE-2011-1870 189 DoS Overflow +Priv Mem. Corr. 2011-07-13 2019-02-26 7.2 None Local Low Not required Complete Complete Complete

Integer overflow in the Client/Server Run-time Subsystem (aka CSRSS) in the Win32 subsystem in Microsoft Windows XP SP2 and SP3, and Windows Server 2003 SP2, allows local users to gain privileges or cause a denial of service (memory corruption) via a crafted application that triggers an incorrect memory assignment for a user transaction, aka "CSRSS Local EOP SrvWriteConsoleOutputString Vulnerability."

38 CVE-2011-1869 399 DoS 2011-06-16 2019-02-26 7.8 None Remote Low Not required None None Complete

The Distributed File System (DFS) implementation in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote DFS servers to cause a denial of service (system hang) via a crafted referral response, aka "DFS Referral Response Vulnerability."

39 CVE-2011-1868 119 Exec Code Overflow Mem. Corr. 2011-06-16 2019-02-26 10.0 None Remote Low Not required Complete Complete Complete

The Distributed File System (DFS) implementation in Microsoft Windows XP SP2 and SP3 and Server 2003 SP2 does not properly validate fields in DFS responses, which allows remote DFS servers to execute arbitrary code via a crafted response, aka "DFS Memory Corruption Vulnerability."

40 CVE-2011-1284 189 DoS Overflow +Priv Mem. Corr. 2011-07-13 2020-09-28 7.2 None Local Low Not required Complete Complete Complete

Integer overflow in the Client/Server Run-time Subsystem (aka CSRSS) in the Win32 subsystem in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges or cause a denial of service (memory corruption) via a crafted application that triggers an incorrect memory assignment for a user transaction, aka "CSRSS Local EOP SrvWriteConsoleOutput Vulnerability."

41 CVE-2011-1283 119 DoS Overflow +Priv Mem. Corr. 2011-07-13 2019-02-26 7.2 None Local Low Not required Complete Complete Complete

The Client/Server Run-time Subsystem (aka CSRSS) in the Win32 subsystem in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, and Windows Server 2008 Gold and SP2 does not ensure that an unspecified array index has a non-negative value before performing read and write operations, which allows local users to gain privileges or cause a denial of service (memory corruption) via a crafted application that triggers an incorrect memory assignment for a user transaction, aka "CSRSS Local EOP SrvSetConsoleNumberOfCommand Vulnerability."

42 CVE-2011-1282 119 DoS Overflow +Priv Mem. Corr. 2011-07-13 2020-09-28 7.2 None Local Low Not required Complete Complete Complete

The Client/Server Run-time Subsystem (aka CSRSS) in the Win32 subsystem in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly initialize memory and consequently uses a NULL pointer in an unspecified function call, which allows local users to gain privileges or cause a denial of service (memory corruption) via a crafted application that triggers an incorrect memory assignment for a user transaction, aka "CSRSS Local EOP SrvSetConsoleLocalEUDC Vulnerability."

43 CVE-2011-1281 119 DoS Overflow +Priv Mem. Corr. 2011-07-13 2020-09-28 7.2 None Local Low Not required Complete Complete Complete

The Client/Server Run-time Subsystem (aka CSRSS) in the Win32 subsystem in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly restrict the number of console objects for a process, which allows local users to gain privileges or cause a denial of service (memory corruption) via a crafted application that triggers an incorrect memory assignment for a user transaction, aka "CSRSS Local EOP AllocConsole Vulnerability."

44 CVE-2011-1268 20 Exec Code 2011-06-16 2020-09-28 10.0 None Remote Low Not required Complete Complete Complete

The SMB client in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote SMB servers to execute arbitrary code via a crafted (1) SMBv1 or (2) SMBv2 response, aka "SMB Response Parsing Vulnerability."

45 CVE-2011-1249 264 +Priv 2011-06-16 2020-09-28 7.2 None Local Low Not required Complete Complete Complete

The Ancillary Function Driver (AFD) in afd.sys in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly validate user-mode input, which allows local users to gain privileges via a crafted application, aka "Ancillary Function Driver Elevation of Privilege Vulnerability."

46 CVE-2011-1247 +Priv 2011-10-12 2020-09-28 9.3 None Remote Medium Not required Complete Complete Complete

Untrusted search path vulnerability in the Microsoft Active Accessibility component in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a Trojan horse DLL in the current working directory, aka "Active Accessibility Insecure Library Loading Vulnerability."

47 CVE-2011-1243 119 Exec Code Overflow 2011-04-13 2018-10-12 9.3 None Remote Medium Not required Complete Complete Complete

The Windows Messenger ActiveX control in msgsc.dll in Microsoft Windows XP SP2 and SP3 allows remote attackers to execute arbitrary code via unspecified vectors that "corrupt the system state," aka "Microsoft Windows Messenger ActiveX Control Vulnerability."

48 CVE-2011-1242 399 +Priv 2011-04-13 2020-09-28 7.2 None Local Low Not required Complete Complete Complete

Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other "Vulnerability Type 1" CVEs listed in MS11-034, aka "Win32k Use After Free Vulnerability."

49 CVE-2011-1241 399 +Priv 2011-04-13 2020-09-28 7.2 None Local Low Not required Complete Complete Complete

Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other "Vulnerability Type 1" CVEs listed in MS11-034, aka "Win32k Use After Free Vulnerability."

50 CVE-2011-1240 399 +Priv 2011-04-13 2020-09-28 7.2 None Local Low Not required Complete Complete Complete

Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other "Vulnerability Type 1" CVEs listed in MS11-034, aka "Win32k Use After Free Vulnerability."