| **Name** | **Description** |
| --- | --- |
| [CVE-2017-8682](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8682) | Windows graphics on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, Windows Server 2016, Microsoft Office Word Viewer, Microsoft Office 2007 Service Pack 3 , and Microsoft Office 2010 Service Pack 2 allows an attacker to execute remote code by the way it handles embedded fonts, aka "Win32k Graphics Remote Code Execution Vulnerability". This CVE ID is unique from CVE-2017-8683. |
| [CVE-2017-8531](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8531) | Graphics in Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, Windows Server 2016, Microsoft Office 2007 Service Pack 3, and Microsoft Office 2010 Service Pack 2 allows improper disclosure of memory contents, aka "Graphics Uniscribe Information Disclosure Vulnerability". This CVE ID is unique from CVE-2017-0286, CVE-2017-0287, CVE-2017-0288, CVE-2017-0289, CVE-2017-8532, and CVE-2017-8533. |
| [CVE-2017-0001](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0001) | The Graphics Device Interface (GDI) in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607 allows local users to gain privileges via a crafted application, aka "Windows GDI Elevation of Privilege Vulnerability." This vulnerability is different from those described in CVE-2017-0005, CVE-2017-0025, and CVE-2017-0047. |
| [CVE-2016-7259](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7259) | The Graphics Component in the kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability." |
| [CVE-2015-7918](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7918) | Multiple buffer overflows in the F1BookView ActiveX control in F1 Bookview in Schneider Electric ProClima before 6.2 allow remote attackers to execute arbitrary code via the (1) Attach, (2) DefinedName, (3) DefinedNameLocal, (4) ODBCPrepareEx, (5) ObjCreatePolygon, (6) SetTabbedTextEx, or (7) SetValidationRule method, a different vulnerability than CVE-2015-8561. |
| [CVE-2015-0093](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0093) | Adobe Font Driver in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to execute arbitrary code via a crafted (1) web site or (2) file, aka "Adobe Font Driver Remote Code Execution Vulnerability," a different vulnerability than CVE-2015-0088, CVE-2015-0090, CVE-2015-0091, and CVE-2015-0092. |
| [CVE-2015-0092](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0092) | Adobe Font Driver in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to execute arbitrary code via a crafted (1) web site or (2) file, aka "Adobe Font Driver Remote Code Execution Vulnerability," a different vulnerability than CVE-2015-0088, CVE-2015-0090, CVE-2015-0091, and CVE-2015-0093. |
| [CVE-2015-0091](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0091) | Adobe Font Driver in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to execute arbitrary code via a crafted (1) web site or (2) file, aka "Adobe Font Driver Remote Code Execution Vulnerability," a different vulnerability than CVE-2015-0088, CVE-2015-0090, CVE-2015-0092, and CVE-2015-0093. |
| [CVE-2015-0090](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0090) | Adobe Font Driver in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to execute arbitrary code via a crafted (1) web site or (2) file, aka "Adobe Font Driver Remote Code Execution Vulnerability," a different vulnerability than CVE-2015-0088, CVE-2015-0091, CVE-2015-0092, and CVE-2015-0093. |
| [CVE-2015-0088](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0088) | Adobe Font Driver in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to execute arbitrary code via a crafted (1) web site or (2) file, aka "Adobe Font Driver Remote Code Execution Vulnerability," a different vulnerability than CVE-2015-0090, CVE-2015-0091, CVE-2015-0092, and CVE-2015-0093. |
| [CVE-2015-0081](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0081) | Windows Text Services (WTS) in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to execute arbitrary code via a crafted (1) web site or (2) file, aka "WTS Remote Code Execution Vulnerability." |
| [CVE-2015-0074](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0074) | Adobe Font Driver in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 does not properly allocate memory, which allows remote attackers to cause a denial of service via a crafted (1) web site or (2) file, aka "Adobe Font Driver Denial of Service Vulnerability." |
| [CVE-2015-0010](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0010) | The CryptProtectMemory function in cng.sys (aka the Cryptography Next Generation driver) in the kernel-mode drivers in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1, when the CRYPTPROTECTMEMORY\_SAME\_LOGON option is used, does not check an impersonation token's level, which allows local users to bypass intended decryption restrictions by leveraging a service that (1) has a named-pipe planting vulnerability or (2) uses world-readable shared memory for encrypted data, aka "CNG Security Feature Bypass Vulnerability" or MSRC ID 20707. |
| [CVE-2014-8499](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8499) | Multiple SQL injection vulnerabilities in ManageEngine Password Manager Pro (PMP) and Password Manager Pro Managed Service Providers (MSP) edition before 7.1 build 7105 allow remote authenticated users to execute arbitrary SQL commands via the SEARCH\_ALL parameter to (1) SQLAdvancedALSearchResult.cc or (2) AdvancedSearchResult.cc. |
| [CVE-2014-4060](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4060) | Use-after-free vulnerability in MCPlayer.dll in Microsoft Windows Media Center TV Pack for Windows Vista, Windows 7 SP1, and Windows Media Center for Windows 8 and 8.1 allows remote attackers to execute arbitrary code via a crafted Office document that triggers deletion of a CSyncBasePlayer object, aka "CSyncBasePlayer Use After Free Vulnerability." |
| [CVE-2014-1884](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1884) | Apache Cordova 3.3.0 and earlier and Adobe PhoneGap 2.9.0 and earlier on Windows Phone 7 and 8 do not properly restrict navigation events, which allows remote attackers to bypass intended device-resource restrictions via content that is accessed (1) in an IFRAME element or (2) with the XMLHttpRequest method by a crafted application. |
| [CVE-2014-0943](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0943) | IBM WebSphere Commerce 6.0 Feature Pack 2 through Feature Pack 5, 7.0.0.0 through 7.0.0.8, and 7.0 Feature Pack 1 through Feature Pack 7 allows remote attackers to cause a denial of service (resource consumption and daemon crash) via a malformed id parameter in a request. |
| [CVE-2013-1712](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1712) | Multiple untrusted search path vulnerabilities in updater.exe in Mozilla Updater in Mozilla Firefox before 23.0, Firefox ESR 17.x before 17.0.8, Thunderbird before 17.0.8, and Thunderbird ESR 17.x before 17.0.8 on Windows 7, Windows Server 2008 R2, Windows 8, and Windows Server 2012 allow local users to gain privileges via a Trojan horse DLL in (1) the update directory or (2) the current working directory. |
| [CVE-2013-1092](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1092) | Multiple unquoted Windows search path vulnerabilities in Novell ZENworks Desktop Management (ZDM) 7 through 7.1 might allow local users to gain privileges via a Trojan horse "program" file in the C: folder, related to an attempted launch of (1) ZenRem32.exe or (2) wm.exe. |
| [CVE-2013-0422](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0422) | Multiple vulnerabilities in Oracle Java 7 before Update 11 allow remote attackers to execute arbitrary code by (1) using the public getMBeanInstantiator method in the JmxMBeanServer class to obtain a reference to a private MBeanInstantiator object, then retrieving arbitrary Class references using the findClass method, and (2) using the Reflection API with recursion in a way that bypasses a security check by the java.lang.invoke.MethodHandles.Lookup.checkSecurityManager method due to the inability of the sun.reflect.Reflection.getCallerClass method to skip frames related to the new reflection API, as exploited in the wild in January 2013, as demonstrated by Blackhole and Nuclear Pack, and a different vulnerability than CVE-2012-4681 and CVE-2012-3174. NOTE: some parties have mapped the recursive Reflection API issue to CVE-2012-3174, but CVE-2012-3174 is for a different vulnerability whose details are not public as of 20130114. CVE-2013-0422 covers both the JMX/MBean and Reflection API issues. NOTE: it was originally reported that Java 6 was also vulnerable, but the reporter has retracted this claim, stating that Java 6 is not exploitable because the relevant code is called in a way that does not bypass security checks. NOTE: as of 20130114, a reliable third party has claimed that the findClass/MBeanInstantiator vector was not fixed in Oracle Java 7 Update 11. If there is still a vulnerable condition, then a separate CVE identifier might be created for the unfixed issue. |
| [CVE-2013-0013](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0013) | The SSL provider component in Microsoft Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, Windows 8, Windows Server 2012, and Windows RT does not properly handle encrypted packets, which allows man-in-the-middle attackers to conduct SSLv2 downgrade attacks against (1) SSLv3 sessions or (2) TLS sessions by intercepting handshakes and injecting content, aka "Microsoft SSL Version 3 and TLS Protocol Security Feature Bypass Vulnerability." |
| [CVE-2012-4774](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4774) | 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 remote attackers to execute arbitrary code via a crafted (1) file name or (2) subfolder name that triggers use of unallocated memory as the destination of a copy operation, aka "Windows Filename Parsing Vulnerability." |
| [CVE-2012-2993](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2993) | Microsoft Windows Phone 7 does not verify the domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof an SSL server for the (1) POP3, (2) IMAP, or (3) SMTP protocol via an arbitrary valid certificate. |
| [CVE-2012-2940](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2940) | MediaChance Real-DRAW PRO 5.2.4 allows remote attackers to cause a denial of service (application crash) via a crafted (1) PNG, (2) WMF, (3) PSD, (4) TGA, (5) TTF, (6) BMP, (7) TIFF, or (8) PCX file. |
| [CVE-2012-0418](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0418) | Unspecified vulnerability in the client in Novell GroupWise 8.0 before Support Pack 3 and 2012 before Support Pack 1 on Windows allows user-assisted remote attackers to execute arbitrary code via a crafted file. |
| [CVE-2012-0180](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0180) | 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, Windows 7 Gold and SP1, and Windows 8 Consumer Preview does not properly handle user-mode input passed to kernel mode for (1) windows and (2) messages, which allows local users to gain privileges via a crafted application, aka "Windows and Messages Vulnerability." |
| [CVE-2012-0175](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0175) | The Shell 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 name for a (1) file or (2) directory, aka "Command Injection Vulnerability." |
| [CVE-2012-0173](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0173) | The Remote Desktop Protocol (RDP) implementation 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 process packets in memory, which allows remote attackers to execute arbitrary code by sending crafted RDP packets triggering access to an object that (1) was not properly initialized or (2) is deleted, aka "Remote Desktop Protocol Vulnerability," a different vulnerability than CVE-2012-0002. |
| [CVE-2012-0156](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0156) | DirectWrite in Microsoft Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly render Unicode characters, which allows remote attackers to cause a denial of service (application hang) via a (1) instant message or (2) web site, aka "DirectWrite Application Denial of Service Vulnerability." |
| [CVE-2012-0002](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0002) | The Remote Desktop Protocol (RDP) implementation 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 process packets in memory, which allows remote attackers to execute arbitrary code by sending crafted RDP packets triggering access to an object that (1) was not properly initialized or (2) is deleted, aka "Remote Desktop Protocol Vulnerability." |
| [CVE-2012-0001](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0001) | The kernel in Microsoft Windows XP SP2, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly load structured exception handling tables, which allows context-dependent attackers to bypass the SafeSEH security feature by leveraging a Visual C++ .NET 2003 application, aka "Windows Kernel SafeSEH Bypass Vulnerability." |
| [CVE-2011-4434](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-4434) | Microsoft Windows Server 2008 R2 and R2 SP1 and Windows 7 Gold and SP1 do not properly enforce AppLocker rules, which allows local users to bypass intended access restrictions via a (1) macro or (2) scripting feature in an application, as demonstrated by Microsoft Office applications and the SANDBOX\_INERT and LOAD\_IGNORE\_CODE\_AUTHZ\_LEVEL flags. |
| [CVE-2011-3330](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3330) | Buffer overflow in the UnitelWay Windows Device Driver, as used in Schneider Electric Unity Pro 6 and earlier, OPC Factory Server 3.34, Vijeo Citect 7.20 and earlier, Telemecanique Driver Pack 2.6 and earlier, Monitor Pro 7.6 and earlier, and PL7 Pro 4.5 and earlier, allows local users, and possibly remote attackers, to execute arbitrary code via an unspecified system parameter. |
| [CVE-2011-2009](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2009) | Untrusted search path vulnerability in Windows Media Center in Microsoft Windows Vista SP2 and Windows 7 Gold and SP1, and Windows Media Center TV Pack for Windows Vista, allows local users to gain privileges via a Trojan horse DLL in the current working directory, aka "Media Center Insecure Library Loading Vulnerability." |
| [CVE-2011-1991](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1991) | 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." |
| [CVE-2011-1268](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1268) | 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." |
| [CVE-2011-1267](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1267) | The SMB server in Microsoft Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote attackers to cause a denial of service (system hang) via a crafted (1) SMBv1 or (2) SMBv2 request, aka "SMB Request Parsing Vulnerability." |
| [CVE-2011-1265](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1265) | The Bluetooth Stack 2.1 in Microsoft Windows Vista SP1 and SP2 and Windows 7 Gold and SP1 does not prevent access to objects in memory that (1) were not properly initialized or (2) have been deleted, which allows remote attackers to execute arbitrary code via crafted Bluetooth packets, aka "Bluetooth Stack Vulnerability." |
| [CVE-2011-1242](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1242) | 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." |
| [CVE-2011-1241](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1241) | 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." |
| [CVE-2011-1240](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1240) | 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." |
| [CVE-2011-1239](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1239) | 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." |
| [CVE-2011-1238](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1238) | 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." |
| [CVE-2011-1237](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1237) | 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." |
| [CVE-2011-1236](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1236) | 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." |
| [CVE-2011-1235](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1235) | 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." |
| [CVE-2011-1234](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1234) | 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." |
| [CVE-2011-0675](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0675) | 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." |
| [CVE-2011-0674](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0674) | 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." |
| [CVE-2011-0672](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0672) | 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." |
| [CVE-2011-0671](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0671) | 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." |
| [CVE-2011-0670](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0670) | 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." |
| [CVE-2011-0667](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0667) | 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." |
| [CVE-2011-0666](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0666) | 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." |
| [CVE-2011-0665](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0665) | 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." |
| [CVE-2011-0662](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0662) | 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." |
| [CVE-2011-0661](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0661) | The SMB Server service 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 fields in SMB requests, which allows remote attackers to execute arbitrary code via a malformed request in a (1) SMBv1 or (2) SMBv2 packet, aka "SMB Transaction Parsing Vulnerability." |
| [CVE-2011-0660](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0660) | 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 Client Response Parsing Vulnerability." |
| [CVE-2011-0657](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0657) | DNSAPI.dll in the DNS 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 does not properly process DNS queries, which allows remote attackers to execute arbitrary code via (1) a crafted LLMNR broadcast query or (2) a crafted application, aka "DNS Query Vulnerability." |
| [CVE-2011-0042](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0042) | SBE.dll in the Stream Buffer Engine in Windows Media Player and Windows Media Center in Microsoft Windows XP SP2 and SP3, Windows XP Media Center Edition 2005 SP3, Windows Vista SP1 and SP2, Windows 7 Gold and SP1, and Windows Media Center TV Pack for Windows Vista does not properly parse Digital Video Recording (.dvr-ms) files, which allows remote attackers to execute arbitrary code via a crafted file, aka "DVR-MS Vulnerability." |
| [CVE-2011-0032](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0032) | Untrusted search path vulnerability in DirectShow in Microsoft Windows Vista SP1 and SP2, Windows 7 Gold and SP1, Windows Server 2008 R2 and R2 SP1, and Windows Media Center TV Pack for Windows Vista allows local users to gain privileges via a Trojan horse DLL in the current working directory, as demonstrated by a directory that contains a Digital Video Recording (.dvr-ms), Windows Recorded TV Show (.wtv), or .mpg file, aka "DirectShow Insecure Library Loading Vulnerability." |
| [CVE-2011-0031](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0031) | The (1) JScript 5.8 and (2) VBScript 5.8 scripting engines in Microsoft Windows Server 2008 R2 and Windows 7 do not properly load decoded scripts obtained from web pages, which allows remote attackers to trigger memory corruption and consequently obtain sensitive information via a crafted web site, aka "Scripting Engines Information Disclosure Vulnerability." |
| [CVE-2010-2744](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2744) | 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, and R2, and Windows 7 do not properly manage a window class, which allows local users to gain privileges by creating a window, then using (1) the SetWindowLongPtr function to modify the popup menu structure, or (2) the SwitchWndProc function with a switch window information pointer, which is not re-initialized when a WM\_NCCREATE message is processed, aka "Win32k Window Class Vulnerability." |
| [CVE-2010-2568](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2568) | Windows Shell in Microsoft Windows XP SP3, Server 2003 SP2, Vista SP1 and SP2, Server 2008 SP2 and R2, and Windows 7 allows local users or remote attackers to execute arbitrary code via a crafted (1) .LNK or (2) .PIF shortcut file, which is not properly handled during icon display in Windows Explorer, as demonstrated in the wild in July 2010, and originally reported for malware that leverages CVE-2010-2772 in Siemens WinCC SCADA systems. |
| [CVE-2010-2551](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2551) | The SMB Server in Microsoft Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 does not properly validate an internal variable in an SMB packet, which allows remote attackers to cause a denial of service (system hang) via a crafted (1) SMBv1 or (2) SMBv2 packet, aka "SMB Variable Validation Vulnerability." |
| [CVE-2010-2191](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2191) | The (1) parse\_str, (2) preg\_match, (3) unpack, and (4) pack functions; the (5) ZEND\_FETCH\_RW, (6) ZEND\_CONCAT, and (7) ZEND\_ASSIGN\_CONCAT opcodes; and the (8) ArrayObject::uasort method in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allow context-dependent attackers to obtain sensitive information (memory contents) or trigger memory corruption by causing a userspace interruption of an internal function or handler. NOTE: vectors 2 through 4 are related to the call time pass by reference feature. |
| [CVE-2010-2138](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2138) | Multiple directory traversal vulnerabilities in ProMan 0.1.1 and earlier allow remote attackers to include and execute arbitrary local files via directory traversal sequences in the \_SESSION[userLang] parameter to (1) elisttasks.php, (2) managepmanagers.php, (3) manageusers.php, (4) helpfunc.php, (5) managegroups.php, (6) manageprocess.php, and (7) manageusersgroups.php. |
| [CVE-2010-0816](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0816) | Integer overflow in inetcomm.dll in Microsoft Outlook Express 5.5 SP2, 6, and 6 SP1; Windows Live Mail on Windows XP SP2 and SP3, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7; and Windows Mail on Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 allows remote e-mail servers and man-in-the-middle attackers to execute arbitrary code via a crafted (1) POP3 or (2) IMAP response, as demonstrated by a certain +OK response on TCP port 110, aka "Outlook Express and Windows Mail Integer Overflow Vulnerability." |
| [CVE-2010-0486](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0486) | The WinVerifyTrust function in Authenticode Signature Verification 5.1, 6.0, and 6.1 in Microsoft Windows 2000 SP4, Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista Gold, SP1, and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 does not properly use unspecified fields in a file digest, which allows user-assisted remote attackers to execute arbitrary code via a modified (1) Portable Executable (PE) or (2) cabinet (aka .CAB) file that incorrectly appears to have a valid signature, aka "WinVerifyTrust Signature Validation Vulnerability." |
| [CVE-2010-0477](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0477) | The SMB client in Microsoft Windows Server 2008 R2 and Windows 7 does not properly handle (1) SMBv1 and (2) SMBv2 response packets, which allows remote SMB servers and man-in-the-middle attackers to execute arbitrary code via a crafted packet that causes the client to read the entirety of the response, and then improperly interact with the Winsock Kernel (WSK), aka "SMB Client Message Size Vulnerability." |
| [CVE-2010-0270](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0270) | The SMB client in Microsoft Windows Server 2008 R2 and Windows 7 does not properly validate fields in SMB transaction responses, which allows remote SMB servers and man-in-the-middle attackers to execute arbitrary code or cause a denial of service (memory corruption and reboot) via a crafted (1) SMBv1 or (2) SMBv2 response, aka "SMB Client Transaction Vulnerability." |
| [CVE-2010-0269](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0269) | The SMB client in Microsoft Windows 2000 SP4, Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista Gold, SP1, and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 does not properly allocate memory for SMB responses, which allows remote SMB servers and man-in-the-middle attackers to execute arbitrary code via a crafted (1) SMBv1 or (2) SMBv2 response, aka "SMB Client Memory Allocation Vulnerability." |
| [CVE-2010-0021](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0021) | Multiple race conditions in the SMB implementation in the Server service in Microsoft Windows Vista Gold, SP1, and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 allow remote attackers to cause a denial of service (system hang) via a crafted (1) SMBv1 or (2) SMBv2 Negotiate packet, aka "SMB Memory Corruption Vulnerability." |
| [CVE-2009-3676](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3676) | The SMB client in the kernel in Microsoft Windows Server 2008 R2 and Windows 7 allows remote SMB servers and man-in-the-middle attackers to cause a denial of service (infinite loop and system hang) via a (1) SMBv1 or (2) SMBv2 response packet that contains (a) an incorrect length value in a NetBIOS header or (b) an additional length field at the end of this response packet, aka "SMB Client Incomplete Response Vulnerability." |
| [CVE-2009-3177](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3177) | Unspecified vulnerability in Kaspersky Online Scanner 7.0 has unknown impact and attack vectors, as demonstrated by a certain module in VulnDisco Pack Professional 8.8, (1) "Kaspersky Online Antivirus Scanner 7.0 exploit (Linux)" and (2) "Kaspersky Online Antivirus Scanner 7.0 exploit (Windows)." NOTE: as of 20090909, this disclosure has no actionable information. However, because the VulnDisco Pack author is a reliable researcher, the issue is being assigned a CVE identifier for tracking purposes. |
| [CVE-2009-3096](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3096) | Multiple unspecified vulnerabilities in HP Performance Insight 5.3 allow remote attackers to have an unknown impact, related to (1) a "Remote exploit" on Windows platforms, and (2) a "Remote preauthentication exploit" on the Windows Server 2003 SP2 platform, as demonstrated by certain modules in VulnDisco Pack Professional 8.11. NOTE: as of 20090903, this disclosure has no actionable information. However, because the VulnDisco Pack author is a reliable researcher, the issue is being assigned a CVE identifier for tracking purposes. |
| [CVE-2009-3089](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3089) | IBM Tivoli Directory Server (TDS) 6.0 allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via unspecified vectors, related to (1) the ibmslapd.exe daemon on Windows and (2) the ibmdiradm daemon in the administration server on Linux, as demonstrated by certain modules in VulnDisco Pack Professional 8.11, a different vulnerability than CVE-2006-0717. NOTE: as of 20090903, this disclosure has no actionable information. However, because the VulnDisco Pack author is a reliable researcher, the issue is being assigned a CVE identifier for tracking purposes. |
| [CVE-2009-2504](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2504) | Multiple integer overflows in unspecified APIs in GDI+ in Microsoft .NET Framework 1.1 SP1, .NET Framework 2.0 SP1 and SP2, Windows XP SP2 and SP3, Windows Server 2003 SP2, Vista Gold and SP1, Server 2008 Gold, Office XP SP3, Office 2003 SP3, 2007 Microsoft Office System SP1 and SP2, Office Project 2002 SP1, Visio 2002 SP2, Office Word Viewer, Word Viewer 2003 Gold and SP3, Office Excel Viewer 2003 Gold and SP3, Office Excel Viewer, Office PowerPoint Viewer 2007 Gold, SP1, and SP2, Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats SP1 and SP2, Expression Web, Expression Web 2, Groove 2007 Gold and SP1, Works 8.5, SQL Server 2000 Reporting Services SP2, SQL Server 2005 SP2 and SP3, Report Viewer 2005 SP1, Report Viewer 2008 Gold and SP1, and Forefront Client Security 1.0 allow remote attackers to execute arbitrary code via (1) a crafted XAML browser application (XBAP), (2) a crafted ASP.NET application, or (3) a crafted .NET Framework application, aka "GDI+ .NET API Vulnerability." |
| [CVE-2009-1531](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1531) | Microsoft Internet Explorer 7 for Windows XP SP2 and SP3; 7 for Server 2003 SP2; 7 for Vista Gold, SP1, and SP2; and 7 for Server 2008 SP2 allows remote attackers to execute arbitrary code via frequent calls to the getElementsByTagName function combined with the creation of an object during reordering of elements, followed by an onreadystatechange event, which triggers an access of an object that (1) was not properly initialized or (2) is deleted, aka "HTML Object Memory Corruption Vulnerability." |
| [CVE-2009-1530](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1530) | Use-after-free vulnerability in Microsoft Internet Explorer 7 for Windows XP SP2 and SP3; 7 for Server 2003 SP2; 7 for Vista Gold, SP1, and SP2; and 7 for Server 2008 SP2 allows remote attackers to execute arbitrary code by repeatedly adding HTML document nodes and calling event handlers, which triggers an access of an object that (1) was not properly initialized or (2) is deleted, aka "HTML Objects Memory Corruption Vulnerability." |
| [CVE-2009-1216](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1216) | Multiple unspecified vulnerabilities in (1) unlzh.c and (2) unpack.c in the gzip libraries in Microsoft Windows Server 2008, Windows Services for UNIX 3.0 and 3.5, and the Subsystem for UNIX-based Applications (SUA); as used in gunzip, gzip, pack, pcat, and unpack 7.x before 7.0.1701.48, 8.x before 8.0.1969.62, and 9.x before 9.0.3790.2076; allow remote attackers to execute arbitrary code via unknown vectors. |
| [CVE-2009-0554](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0554) | Microsoft Internet Explorer 5.01 SP4, 6 SP1, 6 and 7 on Windows XP SP2 and SP3, 6 and 7 on Windows Server 2003 SP1 and SP2, 7 on Windows Vista Gold and SP1, and 7 on Windows Server 2008 allows remote attackers to execute arbitrary code via a web page that triggers presence of an object in memory that was (1) not properly initialized or (2) deleted, aka "Uninitialized Memory Corruption Vulnerability." |
| [CVE-2009-0553](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0553) | Microsoft Internet Explorer 6 SP1, 6 and 7 on Windows XP SP2 and SP3, 6 and 7 on Windows Server 2003 SP1 and SP2, 7 on Windows Vista Gold and SP1, and 7 on Windows Server 2008 allows remote attackers to execute arbitrary code via a web page that triggers presence of an object in memory that was (1) not properly initialized or (2) deleted, aka "Uninitialized Memory Corruption Vulnerability." |
| [CVE-2009-0551](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0551) | Microsoft Internet Explorer 6 SP1, 6 and 7 on Windows XP SP2 and SP3, 6 and 7 on Windows Server 2003 SP1 and SP2, 7 on Windows Vista Gold and SP1, and 7 on Windows Server 2008 does not properly handle transition errors in a request for one HTTP document followed by a request for a second HTTP document, which allows remote attackers to execute arbitrary code via vectors involving (1) multiple crafted pages on a web site or (2) a web page with crafted inline content such as banner advertisements, aka "Page Transition Memory Corruption Vulnerability." |
| [CVE-2009-0243](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0243) | Microsoft Windows does not properly enforce the Autorun and NoDriveTypeAutoRun registry values, which allows physically proximate attackers to execute arbitrary code by (1) inserting CD-ROM media, (2) inserting DVD media, (3) connecting a USB device, and (4) connecting a Firewire device; (5) allows user-assisted remote attackers to execute arbitrary code by mapping a network drive; and allows user-assisted attackers to execute arbitrary code by clicking on (6) an icon under My Computer\Devices with Removable Storage and (7) an option in an AutoPlay dialog, related to the Autorun.inf file. NOTE: vectors 1 and 3 on Vista are already covered by CVE-2008-0951. |
| [CVE-2008-7122](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-7122) | Multiple insecure method vulnerabilities in an ActiveX control in (epRegPro.ocx) in Evans Programming Registry Pro allow remote attackers to read and modify sensitive registry keys via the (1) About, (2) CreateKey, (3) DeleteBranch, (4) DeleteKey, (5) DeleteValue, (6) EnumKeys, (7) EnumValues, (8) QueryType, (9) QueryValue, (10) RenameKey, and (11) SetValue methods. |
| [CVE-2008-6965](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-6965) | AJ Square AJ Auction OOPD, Pro Platinum Skin #1, Pro Platinum Skin #2, and Web 2.0 send a redirect but do not exit when certain scripts are called directly, which allows remote attackers to bypass authentication via a direct request to (1) site.php, (2) auction.php, (3) mail.php, (4) fee\_setting.php, (5) earnings.php, (6) insertion\_fee\_settings.php, (7) custom\_category.php, (8) subcategory.php, (9) category.php, (10) report.php, (11) store\_manager.php, and (12) choose\_sell\_format.php in admin/, and possibly other vectors. |
| [CVE-2008-5877](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5877) | Multiple SQL injection vulnerabilities in Phpclanwebsite (aka PCW) 1.23.3 Fix Pack 5 and earlier, when magic\_quotes\_gpc is disabled, allow remote attackers to execute arbitrary SQL commands via the (1) page parameter to index.php, (2) form\_id parameter to pcw/processforms.php, (3) pcwlogin and (4) pcw\_pass parameters to pcw/setlogin.php, (5) searchvalue parameter to pcw/downloads.php, and the (6) searchvalue and (7) whichfield parameter to pcw/downloads.php, a different vector than CVE-2006-0444. |
| [CVE-2008-3081](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3081) | Multiple unspecified "input validation" vulnerabilities in the Web management interface (aka Messaging Administration interface) in Avaya Message Storage Server (MSS) 3.x and 4.0, and possibly Communication Manager 3.1.x, allow remote authenticated administrators to execute arbitrary commands as user vexvm via vectors related to (1) SFTP Remote Store configuration; (2) remote FTP storage settings; (3) name server lookup; (4) pinging another host; (5) TCP/IP Networking parameter configuration; (6) the external hosts configuration main page; (7) adding and changing external hosts; (8) Windows domain parameter configuration; (9) date, time, and NTP server configuration; (10) alarm settings; (11) the command line history form; (12) the maintenance form; and (13) the server events form. |
| [CVE-2008-2540](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2540) | Apple Safari on Mac OS X, and before 3.1.2 on Windows, does not prompt the user before downloading an object that has an unrecognized content type, which allows remote attackers to place malware into the (1) Desktop directory on Windows or (2) Downloads directory on Mac OS X, and subsequently allows remote attackers to execute arbitrary code on Windows by leveraging an untrusted search path vulnerability in (a) Internet Explorer 7 on Windows XP or (b) the SearchPath function in Windows XP, Vista, and Server 2003 and 2008, aka a "Carpet Bomb" and a "Blended Threat Elevation of Privilege Vulnerability," a different issue than CVE-2008-1032. NOTE: Apple considers this a vulnerability only because the Microsoft products can load application libraries from the desktop and, as of 20080619, has not covered the issue in an advisory for Mac OS X. |
| [CVE-2008-1337](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1337) | The instant message service in Timbuktu Pro 8.6.5 RC 229 and earlier for Windows allows remote attackers to cause (1) a denial of service (daemon crash) via an invalid Version field or (2) a denial of service (CPU consumption and daemon termination) via an invalid or partial message. |
| [CVE-2008-1204](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1204) | Multiple cross-site scripting (XSS) vulnerabilities in the Administration Console in Sun Java System Access Manager 7.1 and 7 2005Q4 allow remote attackers to inject arbitrary web script or HTML via unspecified vectors related to the (1) Help and (2) Version windows. |
| [CVE-2008-1118](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1118) | Timbuktu Pro 8.6.5 for Windows, and possibly 8.7 for Mac OS X, does not perform input validation before logging information fields taken from packets from a remote peer, which allows remote attackers to generate crafted log entries, and possibly avoid detection of attacks, via modified (1) computer name, (2) user name, and (3) IP address fields. |
| [CVE-2008-0583](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0583) | Cross-zone scripting vulnerability in the Internet Explorer web control in Skype 3.6.0.244, and earlier 3.5.x and 3.6.x versions, on Windows allows user-assisted remote attackers to inject arbitrary web script or HTML in the Local Machine Zone via the Description and unspecified other metadata fields of a Metacafe movie submitted by Metacafe Pro to the Skype video gallery, accessible through a search within the (1) "Add video to chat" or (2) "Add video to mood" dialog, a different vector than CVE-2008-0454. |
| [CVE-2008-0207](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0207) | Multiple cross-site scripting (XSS) vulnerabilities in PRO-Search 0.17 and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) prot, (2) host, (3) path, (4) name, (5) ext, (6) size, (7) search\_days, or (8) show\_page parameter to the default URI. |
| [CVE-2007-6553](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6553) | Multiple PHP remote file inclusion vulnerabilities in TeamCal Pro 3.1.000 and earlier allow remote attackers to execute arbitrary PHP code via a URL in the CONF[app\_root] parameter to (1) tcuser.class.php, (2) absencecount.inc.php, (3) avatar.inc.php, (4) csvhandler.class.php, (5) functions.tcpro.php, (6) header.html.inc.php, (7) joomlajack.tcpro.php, (8) menu.inc.php, (9) other.inc.php, (10) tcabsence.class.php, (11) tcabsencegroup.class.php, (12) tcallowance.class.php, (13) tcannouncement.class.php, (14) tcconfig.class.php, (15) tcdaynote.class.php, (16) tcgroup.class.php, (17) tcholiday.class.php, (18) tclogin.class.php, (19) tcmonth.class.php, (20) tctemplate.class.php, (21) tcusergroup.class.php, or (22) tcuseroption.class.php in includes/, possibly a related issue to CVE-2006-4845. |
| [CVE-2007-6017](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6017) | The PVATLCalendar.PVCalendar.1 ActiveX control in pvcalendar.ocx in the scheduler component in the Media Server in Symantec Backup Exec for Windows Server (BEWS) 11d 11.0.6235 and 11.0.7170, and 12.0 12.0.1364, exposes the unsafe Save method, which allows remote attackers to cause a denial of service (browser crash), or create or overwrite arbitrary files, via string values of the (1) \_DOWText0, (2) \_DOWText1, (3) \_DOWText2, (4) \_DOWText3, (5) \_DOWText4, (6) \_DOWText5, (7) \_DOWText6, (8) \_MonthText0, (9) \_MonthText1, (10) \_MonthText2, (11) \_MonthText3, (12) \_MonthText4, (13) \_MonthText5, (14) \_MonthText6, (15) \_MonthText7, (16) \_MonthText8, (17) \_MonthText9, (18) \_MonthText10, and (19) \_MonthText11 properties. NOTE: the vendor states "Authenticated user involvement required," but authentication is not needed to attack a client machine that loads this control. |
| [CVE-2007-6016](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6016) | Multiple stack-based buffer overflows in the PVATLCalendar.PVCalendar.1 ActiveX control in pvcalendar.ocx in the scheduler component in the Media Server in Symantec Backup Exec for Windows Server (BEWS) 11d 11.0.6235 and 11.0.7170, and 12.0 12.0.1364, allow remote attackers to execute arbitrary code via a long (1) \_DOWText0, (2) \_DOWText1, (3) \_DOWText2, (4) \_DOWText3, (5) \_DOWText4, (6) \_DOWText5, (7) \_DOWText6, (8) \_MonthText0, (9) \_MonthText1, (10) \_MonthText2, (11) \_MonthText3, (12) \_MonthText4, (13) \_MonthText5, (14) \_MonthText6, (15) \_MonthText7, (16) \_MonthText8, (17) \_MonthText9, (18) \_MonthText10, or (19) \_MonthText11 property value when executing the Save method. NOTE: the vendor states "Authenticated user involvement required," but authentication is not needed to attack a client machine that loads this control. |
| [CVE-2007-5086](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5086) | Kaspersky Anti-Virus (KAV) and Internet Security 7.0 build 125 do not properly validate certain parameters to System Service Descriptor Table (SSDT) and Shadow SSDT function handlers, which allows local users to cause a denial of service (crash) via the (1) NtUserSendInput, (2) LoadLibraryA, (3) NtOpenProcess, (4) NtOpenThread, (5) NtTerminateProcess, (6) NtUserFindWindowEx, and (7) NtUserBuildHwndList kernel SSDT hooks in kylif.sys; the (8) NtDuplicateObject (DuplicateHandle) kernel SSDT hook; and possibly other kernel SSDT hooks. NOTE: the NtCreateSection vector is covered by CVE-2007-5043.1. NOTE: the vendor disputes that the DuplicateHandle vector is a vulnerability in their code, stating that "it is not an error in our code, but an obscure method for manipulating standard Windows routines to circumvent our self-defense mechanisms." |
| [CVE-2007-5042](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5042) | Outpost Firewall Pro 4.0.1025.7828 does not properly validate certain parameters to System Service Descriptor Table (SSDT) function handlers, which allows local users to cause a denial of service (crash) and possibly gain privileges via the (1) NtCreateKey, (2) NtDeleteFile, (3) NtLoadDriver, (4) NtOpenProcess, (5) NtOpenSection, (6) NtOpenThread, and (7) NtUnloadDriver kernel SSDT hooks, a partial regression of CVE-2006-7160. |
| [CVE-2007-4971](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4971) | ProSecurity 1.40 Beta 2 does not properly validate certain parameters to System Service Descriptor Table (SSDT) function handlers, which allows local users to cause a denial of service (crash) and possibly gain privileges via kernel SSDT hooks for Windows Native API functions including (1) NtCreateKey, (2) NtDeleteFile, (3) NtLoadDriver, (4) NtOpenSection, and (5) NtSetSystemTime. |
| [CVE-2007-4969](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4969) | Process Monitor 1.22 does not properly validate certain parameters to System Service Descriptor Table (SSDT) function handlers, which allows local users to cause a denial of service (crash) and possibly gain privileges via unspecified kernel SSDT hooks for Windows Native API functions including (1) NtCreateKey, (2) NtDeleteValueKey, (3) NtLoadKey, (4) NtOpenKey, (5) NtQueryValueKey, (6) NtSetValueKey, and (7) NtUnloadKey. |
| [CVE-2007-4967](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4967) | Online Armor Personal Firewall 2.0.1.215 does not properly validate certain parameters to System Service Descriptor Table (SSDT) function handlers, which allows local users to cause a denial of service (crash) and possibly gain privileges via unspecified kernel SSDT hooks for Windows Native API functions including (1) NtAllocateVirtualMemory, (2) NtConnectPort, (3) NtCreateFile, (4) NtCreateKey, (5) NtCreatePort, (6) NtDeleteFile, (7) NtDeleteValueKey, (8) NtLoadKey, (9) NtOpenFile, (10) NtOpenProcess, (11) NtOpenThread, (12) NtResumeThread, (13) NtSetContextThread, (14) NtSetValueKey, (15) NtSuspendProcess, (16) NtSuspendThread, and (17) NtTerminateThread. |
| [CVE-2007-4841](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4841) | Mozilla Firefox before 2.0.0.8, Thunderbird before 2.0.0.8, and SeaMonkey before 1.1.5 allows remote attackers to execute arbitrary commands via a (1) mailto, (2) nntp, (3) news, or (4) snews URI with invalid "%" encoding, related to improper file type handling on Windows XP with Internet Explorer 7 installed, a variant of CVE-2007-3845. |
| [CVE-2007-4790](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4790) | Stack-based buffer overflow in certain ActiveX controls in (1) FPOLE.OCX 6.0.8450.0 and (2) Foxtlib.ocx, as used in the Microsoft Visual FoxPro 6.0 fpole 1.0 Type Library; and Internet Explorer 5.01, 6 SP1 and SP2, and 7; allows remote attackers to execute arbitrary code via a long first argument to the FoxDoCmd function. |
| [CVE-2007-4412](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4412) | Multiple cross-site scripting (XSS) vulnerabilities in Headstart Solutions DeskPRO 3.0.2 allow remote authenticated users to inject arbitrary web script or HTML via unspecified parameters to (1) techs.php, (2) ticket\_category.php, (3) ticket\_priority.php, (4) ticket\_workflow.php, (5) ticket\_escalate.php, (6) fields\_ticket.php, (7) ticket\_rules\_web.php, (8) ticket\_displayfields.php, (9) ticket\_rules\_mail.php, (10) fields\_user.php, (11) fields\_faq.php, and (12) user\_help.php, in (a) admincp/ and (b) possibly a directory on the "User side." |
| [CVE-2007-4221](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4221) | Multiple buffer overflows in Motorola Timbuktu Pro before 8.6.5 for Windows allow remote attackers to cause a denial of service (daemon crash) or possibly execute arbitrary code via (1) a long user name and (2) certain malformed requests; and (3) allow remote Timbuktu servers to have an unknown impact via a malformed HELLO response, related to the Scanner component and possibly related to a malformed computer name. |
| [CVE-2007-4220](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4220) | Directory traversal vulnerability in Motorola Timbuktu Pro before 8.6.5 for Windows allows remote attackers to create or delete arbitrary files via a .. (dot dot) in a Send request, probably related to the (1) Send and (2) Exchange services. |
| [CVE-2007-4218](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4218) | Multiple buffer overflows in the ServerProtect service (SpntSvc.exe) in Trend Micro ServerProtect for Windows before 5.58 Security Patch 4 allow remote attackers to execute arbitrary code via certain RPC requests to certain TCP ports that are processed by the (1) RPCFN\_ENG\_NewManualScan, (2) RPCFN\_ENG\_TimedNewManualScan, and (3) RPCFN\_SetComputerName functions in (a) StRpcSrv.dll; the (4) RPCFN\_CMON\_SetSvcImpersonateUser and (5) RPCFN\_OldCMON\_SetSvcImpersonateUser functions in (b) Stcommon.dll; the (6) RPCFN\_ENG\_TakeActionOnAFile and (7) RPCFN\_ENG\_AddTaskExportLogItem functions in (c) Eng50.dll; the (8) NTF\_SetPagerNotifyConfig function in (d) Notification.dll; or the (9) RPCFN\_CopyAUSrc function in the (e) ServerProtect Agent service. |
| [CVE-2007-4081](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4081) | Multiple cross-site scripting (XSS) vulnerabilities in AlstraSoft Affiliate Network Pro allow remote attackers to inject arbitrary web script or HTML via vectors in (a) merchants/index.php, including the (1) id or (2) msg parameter in a programedit action; the (3) pgmid parameter in an uploadProducts action; the (4) d, (5) m, or (6) y parameter in a daily action; the (7) err parameter in a ProgramReport action; the (8) i, (9) txtto, (10) txtfrom, or (11) programs parameter in a LinkReport action; or the (12) msg parameter in an add\_money action; and one vector in (b) merchants/temp.php using (13) the rowid parameter. NOTE: vector 7 might overlap CVE-2005-3795.1. |
| [CVE-2007-2326](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2326) | Multiple PHP remote file inclusion vulnerabilities in HYIP Manager Pro allow remote attackers to execute arbitrary PHP code via a URL in the plugin\_file parameter to (1) Smarty.class.php and (2) Smarty\_Compiler.class.php in inc/libs/; (3) core.display\_debug\_console.php, (4) core.load\_plugins.php, (5) core.load\_resource\_plugin.php, (6) core.process\_cached\_inserts.php, (7) core.process\_compiled\_include.php, and (8) core.read\_cache\_file.php in inc/libs/core/; and other unspecified files. NOTE: (1) and (2) might be incorrectly reported vectors in Smarty. |
| [CVE-2007-1119](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1119) | Unspecified vulnerability in Novell ZENworks 7 Desktop Management Support Pack 1 before Hot patch 3 (ZDM7SP1HP3) allows remote attackers to upload images to certain folders that were not configured in the "Only allow uploads to the following directories" setting via unspecified vectors. |
| [CVE-2007-0612](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0612) | Multiple ActiveX controls in Microsoft Windows 2000, XP, 2003, and Vista allows remote attackers to cause a denial of service (Internet Explorer crash) by accessing the bgColor, fgColor, linkColor, alinkColor, vlinkColor, or defaultCharset properties in the (1) giffile, (2) htmlfile, (3) jpegfile, (4) mhtmlfile, (5) ODCfile, (6) pjpegfile, (7) pngfile, (8) xbmfile, (9) xmlfile, (10) xslfile, or (11) wdfile objects in (a) mshtml.dll; or the (12) TriEditDocument.TriEditDocument or (13) TriEditDocument.TriEditDocument.1 objects in (b) triedit.dll, which cause a NULL pointer dereference. |
| [CVE-2007-0018](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0018) | Stack-based buffer overflow in the NCTAudioFile2.AudioFile ActiveX control (NCTAudioFile2.dll), as used by multiple products, allows remote attackers to execute arbitrary code via a long argument to the SetFormatLikeSample function. NOTE: the products include (1) NCTsoft NCTAudioStudio, NCTAudioEditor, and NCTDialogicVoice; (2) Magic Audio Recorder, Music Editor, and Audio Converter; (3) Aurora Media Workshop; DB Audio Mixer And Editor; (4) J. Hepple Products including Fx Audio Editor and others; (5) EXPStudio Audio Editor; (6) iMesh; (7) Quikscribe; (8) RMBSoft AudioConvert and SoundEdit Pro 2.1; (9) CDBurnerXP; (10) Code-it Software Wave MP3 Editor and aBasic Editor; (11) Movavi VideoMessage, DVD to iPod, and others; (12) SoftDiv Software Dexster, iVideoMAX, and others; (13) Sienzo Digital Music Mentor (DMM); (14) MP3 Normalizer; (15) Roemer Software FREE and Easy Hi-Q Recorder, and Easy Hi-Q Converter; (16) Audio Edit Magic; (17) Joshua Video and Audio Converter; (18) Virtual CD; (19) Cheetah CD and DVD Burner; (20) Mystik Media AudioEdit Deluxe, Blaze Media, and others; (21) Power Audio Editor; (22) DanDans Digital Media Full Audio Converter, Music Editing Master, and others; (23) Xrlly Software Text to Speech Makerand Arial Sound Recorder / Audio Converter; (24) Absolute Sound Recorder, Video to Audio Converter, and MP3 Splitter; (25) Easy Ringtone Maker; (26) RecordNRip; (27) McFunSoft iPod Audio Studio, Audio Recorder for Free, and others; (28) MP3 WAV Converter; (29) BearShare 6.0.2.26789; and (30) Oracle Siebel SimBuilder and CRM 7.x. |
| [CVE-2006-7160](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-7160) | The Sandbox.sys driver in Outpost Firewall PRO 4.0, and possibly earlier versions, does not validate arguments to hooked SSDT functions, which allows local users to cause a denial of service (crash) via invalid arguments to the (1) NtAssignProcessToJobObject,, (2) NtCreateKey, (3) NtCreateThread, (4) NtDeleteFile, (5) NtLoadDriver, (6) NtOpenProcess, (7) NtProtectVirtualMemory, (8) NtReplaceKey, (9) NtTerminateProcess, (10) NtTerminateThread, (11) NtUnloadDriver, and (12) NtWriteVirtualMemory functions. |
| [CVE-2006-7000](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-7000) | Headstart Solutions DeskPRO allows remote attackers to obtain the full path via direct requests to (1) email/mail.php, (2) includes/init.php, (3) certain files in includes/cron/, and (4) jpgraph.php, (5) jpgraph\_bar.php, (6) jpgraph\_pie.php, and (7) jpgraph\_pie3d.php in includes/graph/, which leaks the path in error messages. |
| [CVE-2006-6974](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6974) | Headstart Solutions DeskPRO stores sensitive information under the web root with insufficient access control, which allows remote attackers to (1) list files in the includes/ directory; obtain the SQL username and password via a direct request for (2) config.php and (3) config.php.bak in includes/; read files in (4) email/, (5) admin/graphs/, (6) includes/javascript/, and (7) certain other includes/ directories via direct requests; and download SQL database data via direct requests for (8) data.sql, (9) install.sql, (10) settings.sql, and possibly other files in install/v2data/. |
| [CVE-2006-6518](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6518) | Multiple cross-site scripting (XSS) vulnerabilities in ProNews 1.5 allow remote attackers to inject arbitrary web script or HTML via the (1) pseudo, (2) email, (3) date, (4) sujet, (5) message, (6) site, and (7) lien parameters to (a) admin/change.php, and the (8) aa parameter to (b) lire-avis.php. |
| [CVE-2006-5904](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5904) | Multiple PHP remote file inclusion vulnerabilities in MWChat Pro 7.0 allow remote attackers to execute arbitrary PHP code via a URL in the CONFIG[MWCHAT\_Libs] parameter to (1) about.php, (2) buddy.php, (3) chat.php, (4) dialog.php, (5) head.php, (6) help.php, (7) index.php, and (8) license.php, different vectors than CVE-2005-1869. |
| [CVE-2006-5143](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5143) | Multiple buffer overflows in CA BrightStor ARCserve Backup r11.5 SP1 and earlier, r11.1, and 9.01; BrightStor ARCserve Backup for Windows r11; BrightStor Enterprise Backup 10.5; Server Protection Suite r2; and Business Protection Suite r2 allow remote attackers to execute arbitrary code via crafted data on TCP port 6071 to the Backup Agent RPC Server (DBASVR.exe) using the RPC routines with opcode (1) 0x01, (2) 0x02, or (3) 0x18; invalid stub data on TCP port 6503 to the RPC routines with opcode (4) 0x2b or (5) 0x2d in ASCORE.dll in the Message Engine RPC Server (msgeng.exe); (6) a long hostname on TCP port 41523 to ASBRDCST.DLL in the Discovery Service (casdscsvc.exe); or unspecified vectors related to the (7) Job Engine Service. |
| [CVE-2006-4969](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4969) | Multiple PHP remote file inclusion vulnerabilities in WAHM E-Commerce Pie Cart Pro allow remote attackers to execute arbitrary PHP code via a URL in the Inc\_Dir parameter in (1) affiliates.php, (2) orders.php, (3) events.php, (4) index.php, (5) articles.php, (6) faqs.php, (7) guestbook.php, (8) catalog.php, (9) wholesale.php, (10) weblinks.php, (11) certificates.php, (12) sitesearch.php, (13) contact.php, (14) sitemap.php, (15) search.php, (16) registry.php, or (17) error.php. |
| [CVE-2006-4220](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4220) | Multiple cross-site scripting (XSS) vulnerabilities in webacc in Novell GroupWise WebAccess before 7 Support Pack 3 Public Beta allow remote attackers to inject arbitrary web script or HTML via the (1) User.html, (2) Error, (3) User.Theme.index, and (4) and User.lang parameters. |
| [CVE-2006-3992](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3992) | Unspecified vulnerability in the Centrino (1) w22n50.sys, (2) w22n51.sys, (3) w29n50.sys, and (4) w29n51.sys Microsoft Windows drivers for Intel 2200BG and 2915ABG PRO/Wireless Network Connection before 10.5 with driver 9.0.4.16 allows remote attackers to execute arbitrary code via certain frames that trigger memory corruption. |
| [CVE-2006-3697](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3697) | Agnitum Outpost Firewall Pro 3.51.759.6511 (462), as used in (1) Lavasoft Personal Firewall 1.0.543.5722 (433) and (2) Novell BorderManager Novell Client Firewall 2.0, does not properly restrict user activities in application windows that run in a LocalSystem context, which allows local users to gain privileges and execute commands (a) via the "open folder" option when no instance of explorer.exe is running, possibly related to the ShellExecute API function; or (b) by overwriting a batch file through the "Save Configuration As" option. NOTE: this might be a vulnerability in Microsoft Windows and explorer.exe instead of the firewall. |
| [CVE-2006-3074](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3074) | klif.sys in Kaspersky Internet Security 6.0 and 7.0, Kaspersky Anti-Virus (KAV) 6.0 and 7.0, KAV 6.0 for Windows Workstations, and KAV 6.0 for Windows Servers does not validate certain parameters to the (1) NtCreateKey, (2) NtCreateProcess, (3) NtCreateProcessEx, (4) NtCreateSection, (5) NtCreateSymbolicLinkObject, (6) NtCreateThread, (7) NtDeleteValueKey, (8) NtLoadKey2, (9) NtOpenKey, (10) NtOpenProcess, (11) NtOpenSection, and (12) NtQueryValueKey hooked system calls, which allows local users to cause a denial of service (reboot) via an invalid parameter, as demonstrated by the ClientId parameter to NtOpenProcess. |
| [CVE-2006-2094](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2094) | Microsoft Internet Explorer before Windows XP Service Pack 2 and Windows Server 2003 Service Pack 1, when Prompt is configured in Security Settings, uses modal dialogs to verify that a user wishes to run an ActiveX control or perform other risky actions, which allows user-assisted remote attackers to construct a race condition that tricks a user into clicking an object or pressing keys that are actually applied to a "Yes" approval for executing the control. |
| [CVE-2006-1965](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1965) | Multiple cross-site scripting (XSS) vulnerabilities in aasi media Net Clubs Pro 4.0 and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) onuser, (2) pass, (3) chatsys, (4) room, (5) username, and (6) to parameters in (a) sendim.cgi; the (7) username parameter in (b) imessage.cgi; the (8) password parameter in (c) login.cgi; and the (9) cat\_id parameter in (d) viewcat.cgi. |
| [CVE-2006-1278](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1278) | SQL injection vulnerability in @1 File Store 2006.03.07 allows remote attackers to execute arbitrary SQL commands via the id parameter to (1) functions.php and (2) user.php in the libs directory, (3) edit.php and (4) delete.php in control/files/, (5) edit.php and (6) delete.php in control/users/, (7) edit.php, (8) access.php, and (9) in control/folders/, (10) access.php and (11) delete.php in control/groups/, (12) confirm.php, and (13) download.php; (14) the email parameter in password.php, and (15) the id parameter in folder.php. NOTE: it was later reported that vectors 12 and 13 also affect @1 File Store PRO 3.2. |
| [CVE-2005-4243](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-4243) | Multiple SQL injection vulnerabilities in QuickPayPro 3.1 allow remote attackers to execute arbitrary SQL commands via the (1) popupid parameter in popups.edit.php; (2) so, (3) sb, and (4) nr parameters in customer.tickets.view.php; (5) subrackingid parameter in subscribers.tracking.edit.php; (6) delete parameter in design.php; (7) trackingid parameter in tracking.details.php; and (8) customerid parameter in sales.view.php. |
| [CVE-2005-3976](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3976) | SQL injection vulnerability in type.asp, as used in multiple DUware products including (1) DUamazon 3.1, (2) DUarticle 1.1, (3) DUclassified 4.2, (4) DUdirectory 3.1 and DUdirectory Pro 3.0 and 3.0 SQL, (5) DUdownload 1.1, (6) DUgallery 3.3, (7) DUnews 1.1, and (8) DUpaypal 3.1 and DUpaypal Pro 3.0, allows remote attackers to execute arbitrary SQL commands via the iType parameter. |
| [CVE-2005-2865](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-2865) | Multiple PHP remote file inclusion vulnerabilities in aMember Pro 2.3.4 allow remote attackers to execute arbitrary PHP code via the config[root\_dir] parameter to (1) mysql.inc.php, (2) efsnet.inc.php, (3) theinternetcommerce.inc.php, (4) cdg.inc.php, (5) compuworld.inc.php, (6) directone.inc.php, (7) authorize\_aim.inc.php, (8) beanstream.inc.php, (9) config.inc.php, (10) eprocessingnetwork.inc.php, (11) eway.inc.php, (12) linkpoint.inc.php, (13) logiccommerce.inc.php, (14) netbilling.inc.php, (15) payflow\_pro.inc.php, (16) paymentsgateway.inc.php, (17) payos.inc.php, (18) payready.inc.php, or (19) plugnplay.inc.php. |
| [CVE-2005-2840](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-2840) | Multiple unknown vulnerabilities in MAXdev MD-Pro 1.0.72 and earlier have unknown impact and unspecified attack vectors, in one or more of the (1) Download, (2) Search, (3) Web links, (4) Blocks, (5) Messages, (6) News, (7) Comments, (8) Settings, (9) Stats or (10) subjects modules. |
| [CVE-2005-2046](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-2046) | Multiple SQL injection vulnerabilities in DUware DUamazon Pro 3.0 and 3.1 allow remote attackers to execute arbitrary SQL commands via the (1) iCat parameter to cat.asp, (2) iSub parameter to sub.asp, (3) iSub parameter to detail.asp, (4) iPro parameter to review.asp, iCat parameter to (5) catEdit.asp, (6) catDelete.asp, (7) productEdit.asp, or (8) productDelete.asp, or (9) iType parameter to type.asp. |
| [CVE-2005-1983](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-1983) | Stack-based buffer overflow in the Plug and Play (PnP) service for Microsoft Windows 2000 and Windows XP Service Pack 1 allows remote attackers to execute arbitrary code via a crafted packet, and local users to gain privileges via a malicious application, as exploited by the Zotob (aka Mytob) worm. |
| [CVE-2005-1224](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-1224) | Multiple SQL injection vulnerabilities in DUware DUportal Pro 3.4 allow remote attackers to execute arbitrary SQL commands via the (1) nChannel parameter to default.asp, cat.asp, or detail.asp, (2) the iChannel parameter to search.asp, default.asp, result.asp, cat.asp, or detail.asp (3) the iCat parameter to cat.asp or detail.asp, (4) the iData parameter to detail.asp or result.asp, the (5) POL\_ID, (6) POL\_PARENT, (7) POL\_CATEGORY, (8) CHA\_NAME, or (9) CHA\_ID parameters to inc\_vote.asp, or the (10) tfm\_order or (11) tfm\_orderby parameters to toppages.asp, a different set of vulnerabilities than CVE-2005-1236. |
| [CVE-2005-0928](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-0928) | Multiple cross-site scripting (XSS) vulnerabilities in PhotoPost PHP Pro 5.x allow remote attackers to inject arbitrary web script or HTML via the (1) cat, (2) password, (3) ppuser, (4) sort, or (5) si parameters to showgallery.php, the (6) ppuser, (7) sort, or (8) si parameters to showmembers.php, or (9) the photo parameter to slideshow.php. |
| [CVE-2005-0083](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-0083) | MySQL MaxDB 7.5.00 for Windows, and possibly earlier versions and other platforms, allows remote attackers to cause a denial of service (application crash) via invalid parameters to the (1) DBMCli\_String::ReallocString, (2) DBMCli\_String::operator, (3) DBMCli\_Buffer::ForceResize, (4) DBMCli\_Wizard::InstallDatabase, (5) DBMCli\_Devspaces::Complete, (6) DBMWeb\_TemplateWizard::askForWriteCountStep5, or (7) DBMWeb\_DBMWeb::wizardDB functions, which triggers a null dereference. |
| [CVE-2004-1871](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-1871) | Multiple cross-site scripting (XSS) vulnerabilities in PhotoPost PHP Pro 4.6.x and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) ppuser, (2) password, (3) stype, (4) perpage, (5) sort, (6) page, (7) si, or (8) cat parameters to showmembers.php, or the (9) photo name, (10) photo description, (11) album name, or (12) album description fields. |
| [CVE-2004-1870](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-1870) | Multiple SQL injection vulnerabilities in PhotoPost PHP Pro 4.6.x and earlier allow remote attackers to gain users' passwords via the (1) photo parameter to addfav.php, (2) photo parameter to comments.php, (3) credit parameter to comments.php, (4) cat parameter to index.php, (5) ppuser parameter to showgallery.php, (6) cat parameter to showgallery.php, (7) cat parameter to uploadphoto.php, (8) albumid parameter to useralbums.php, or (9) albumid parameter to useralbums.php. |
| [CVE-2002-2407](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-2407) | Certain patches for QNX Neutrino realtime operating system (RTOS) 6.2.0 set insecure permissions for the files (1) /sbin/io-audio by OS Update Patch A, (2) /bin/shutdown, (3) /sbin/fs-pkg, and (4) phshutdown by QNX experimental patches, (5) cpim, (6) vpim, (7) phrelaycfg, and (8) columns, (9) othello, (10) peg, (11) solitaire, and (12) vpoker in the games pack 2.0.3, which allows local users to gain privileges by modifying the files before permissions are changed. |
| [CVE-2002-0370](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0370) | Buffer overflow in the ZIP capability for multiple products allows remote attackers to cause a denial of service or execute arbitrary code via ZIP files containing entries with long filenames, including (1) Microsoft Windows 98 with Plus! Pack, (2) Windows XP, (3) Windows ME, (4) Lotus Notes R4 through R6 (pre-gold), (5) Verity KeyView, and (6) Stuffit Expander before 7.0. |
| [CVE-2001-0242](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0242) | Buffer overflows in Microsoft Windows Media Player 7 and earlier allow remote attackers to execute arbitrary commands via (1) a long version tag in an .ASX file, or (2) a long banner tag, a variant of the ".ASX Buffer Overrun" vulnerability as discussed in MS:MS00-090. |