CVE-ID	Vuln Description	Access Vector	Attack Complexity	Privileges Required	User Interaction	C Impact	I Impact	A Impact	Estimated Score	Confident?	User comments
CVE-2009-0927	Stack-based buffer overflow in Adobe Reader and Adobe Acrobat 9 before 9.1, 8 before 8.1.3 , and 7 before 7.1.1 allows remote attackers to execute arbitrary code via a crafted argument to the getIcon method of a Collab object, a different vulnerability than CVE-2009-0658.										
CVE-2009-1862	Unspecified vulnerability in Adobe Reader and Acrobat 9.x through 9.1.2, and Adobe Flash Player 9.x through 9.0.159.0 and 10.x through 10.0.22.87, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via (1) a crafted Flash application in a .pdf file or (2) a crafted .swf file, related to authplay.dll, as exploited in the wild in July 2009.										
CVE-2013-1956	Linux Kernel contains a flaw in fs/namespace.c that leads to unauthorized privileges being gained. By utilizing a chrooted program, a local attacker can create a new user namespace and mount namesapce. This may allow the attacker to gain elevated privileges by escaping the new root via a persisting file descriptor.										
CVE-2011-4696	Eye-Fi Helper contains a flaw that allows an attacker to traverse outside of a restricted path. The issue is due to the program not properly sanitizing user input, specifically directory traversal style attacks (e.g., ../../) during the handling of .tar image files. This directory traversal attack would allow a remote attacker to write to arbitrary files and gain escalated privileges.										
CVE-2009-1136	The Microsoft Office Web Components Spreadsheet ActiveX control (aka OWC10 or OWC11), as distributed in Office XP SP3 and Office 2003 SP3, Office XP Web Components SP3, Office 2003 Web Components SP3, Office 2003 Web Components SP1 for the 2007 Microsoft Office System, Internet Security and Acceleration (ISA) Server 2004 SP3 and 2006 Gold and SP1, and Office Small Business Accounting 2006, when used in Internet Explorer, allows remote attackers to execute arbitrary code via a crafted call to the msDataSourceObject method, as exploited in the wild in July and August 2009, aka "Office Web Components HTML Script Vulnerability."										
CVE-2009-3873	The JPEG Image Writer in Sun Java SE in JDK and JRE 5.0 before Update 22, JDK and JRE 6 before Update 17, and SDK and JRE 1.4.x before 1.4.2_24 allows remote attackers to gain privileges via a crafted image file, related to a "quantization problem," aka Bug Id 6862968.										
CVE-2009-1107	The Java Plug-in in Java SE Development Kit (JDK) and Java Runtime Environment (JRE) 6 Update 12 and earlier, and 5.0 Update 17 and earlier, allows remote attackers to trick a user into trusting a signed applet via unknown vectors that misrepresent the security warning dialog, related to a "Swing JLabel HTML parsing vulnerability," aka CR 6782871.										
CVE-2009-3762	Unspecified vulnerability in Oracle OpenSSO Enterprise 8.0 allows remote attackers to affect integrity via unknown vectors.										
CVE-2010-0483	vbscript.dll in VBScript 5.1, 5.6, 5.7, and 5.8 in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2, when Internet Explorer is used, allows user-assisted remote attackers to execute arbitrary code by referencing a (1) local pathname, (2) UNC share pathname, or (3) WebDAV server with a crafted .hlp file in the fourth argument (aka helpfile argument) to the MsgBox function, leading to code execution involving winhlp32.exe when the F1 key is pressed, aka "VBScript Help Keypress Vulnerability."										
CVE-2012-0507	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 2 and earlier, 6 Update 30 and earlier, and 5.0 Update 33 and earlier allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Concurrency. NOTE: the previous information was obtained from the February 2012 Oracle CPU. Oracle has not commented on claims from a downstream vendor and third party researchers that this issue occurs because the AtomicReferenceArray class implementation does not ensure that the array is of the Object[] type, which allows attackers to cause a denial of service (JVM crash) or bypass Java sandbox restrictions. NOTE: this issue was originally mapped to CVE-2011-3571, but that identifier was already assigned to a different issue.										
CVE-2009-2409	The Network Security Services (NSS) library before 3.12.3, as used in Firefox; GnuTLS before 2.6.4 and 2.7.4; OpenSSL 0.9.8 through 0.9.8k; and other products support MD2 with X.509 certificates, which might allow remote attackers to spoof certificates by using MD2 design flaws to generate a hash collision in less than brute-force time. NOTE: the scope of this issue is currently limited because the amount of computation required is still large.										
CVE-2010-3974	fxscover.exe in the Fax Cover Page Editor 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 parse FAX cover pages, which allows remote attackers to execute arbitrary code via a crafted .cov file, aka "Fax Cover Page Editor Memory Corruption Vulnerability."										
CVE-2011-2140	Adobe Flash Player before 10.3.183.5 on Windows, Mac OS X, Linux, and Solaris and before 10.3.186.3 on Android, and Adobe AIR before 2.7.1 on Windows and Mac OS X and before 2.7.1.1961 on Android, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-2135, CVE-2011-2417, and CVE-2011-2425.										
CVE-2013-4695	Winamp contains a flaw in the gen_ff.dll library. The issue is triggered when handling the '&lt;link name&gt;' and '&lt;home url&gt;' key values, which will result in a pointer dereference. This may allow a context-dependent attacker to execute arbitrary code.										
CVE-2013-0375	A vulnerability in earlier versions of the MySQL Server database could allow a remote, authenticated user to inject SQL code that MySQL replication functionality would run with high privileges. A successful attack could allow any data in the MySQL database to be read or modified.										
CVE-2014-2005	Sophos Disk Encryption (SDE) 5.x in Sophos Enterprise Console (SEC) 5.x before 5.2.2 does not enforce intended authentication requirements for a resume action from sleep mode, which allows physically proximate attackers to obtain desktop access by leveraging the absence of a login screen.										
CVE-2014-0160	The (1) TLS and (2) DTLS implementations in OpenSSL 1.0.1 before 1.0.1g do not properly handle Heartbeat Extension packets, which allows remote attackers to obtain sensitive information from process memory via crafted packets that trigger a buffer over-read, as demonstrated by reading private keys, related to d1_both.c and t1_lib.c, aka the Heartbleed bug.										
CVE-2013-0792	Mozilla Firefox before 20.0 and SeaMonkey before 2.17, when gfx.color_management.enablev4 is used, do not properly handle color profiles during PNG rendering, which allows remote attackers to obtain sensitive information from process memory or cause a denial of service (memory corruption) via a grayscale PNG image.										

CVE-ID	Vuln Description	Access Vector	Attack Complexity	Privileges Required	User Interaction	C Impact	I Impact	A Impact	Estimated Score	Confident?	User comments
CVE-2013-5173	Apple Mac OS X contains a flaw that may allow a local denial of service. The issue is due to the kernel random number generator holding a lock while performing requests from userspace. This may allow a local attacker to cause the system to prevent other applications from gaining the entropy needed for a long period of time, undermining RNG-based functions.										
CVE-2013-6014	If Proxy ARP is enabled on an unnumbered interface, an attacker can poison the ARP cache and create a bogus forwarding table entry for an IP address, effectively creating a denial of service for that subscriber or interface. When Proxy ARP is enabled on an unnumbered interface, the router will answer any ARP message from any IP address which could lead to exploitable information disclosure. This issue can affect any product or platform running Junos OS 10.4, 11.4, 11.4X27, 12.1, 12.1X44, 12.1X45, 12.2, 12.3, or 13.1, supporting unnumbered interfaces.										
CVE-2013-0224	Video Module for Drupal contains a flaw that is triggered during the handling of content within temporary PHP files. This may allow a remote attacker to inject arbitrary code in to the temporary PHP file, which will cause the code to be executed by the program when the file is read.										
CVE-2010-0840	Unspecified vulnerability in the Java Runtime Environment component in Oracle Java SE and Java for Business 6 Update 18, 5.0 Update 23, and 1.4.2_25 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors. NOTE: the previous information was obtained from the March 2010 CPU. Oracle has not commented on claims from a reliable researcher that this is related to improper checks when executing privileged methods in the Java Runtime Environment (JRE), which allows attackers to execute arbitrary code via (1) an untrusted object that extends the trusted class but has not modified a certain method, or (2) "a similar trust issue with interfaces," aka "Trusted Methods Chaining Remote Code Execution Vulnerability."										
CVE-2010-3066	The io_submit_one function in fs/aio.c in the Linux kernel before 2.6.23 allows local users to cause a denial of service (NULL pointer dereference) via a crafted io_submit system call with an IOCB_FLAG_RESFD flag.										
CVE-2013-0086	Microsoft OneNote contains a flaw that may lead to unauthorized disclosure of potentially sensitive information. The issue is triggered when allocating memory when validating buffer sizes during the handling of a specially crafted ONE file. This may allow a context-dependent attacker to gain access to potentially sensitive information.										
CVE-2013-6182	EMC Replication Manager contains a flaw that leads to unauthorized privileges being gained. The issue is triggered when handling a specially crafted path that contains unquoted elements such as white space or other separators. This may allow a local attacker to gain elevated privileges.										
CVE-2013-4251	SciPy contains a flaw in the scipy.weave component that leads to unauthorized privileges being gained. The issue is due to the program insecurely creating temporary directories, this may allow a local attacker to inject code in to a directory to be executed with user privileges, which can allow the attacker to gain elevated privileges.										
CVE-2007-6195	Buffer overflow in the sw_rpc_agent_init function in swagentd in Software Distributor (SD), and possibly other DCE applications, in HP HP-UX B.11.11 and B.11.23 allows remote attackers to execute arbitrary code or cause a denial of service via malformed arguments in an opcode 0x04 DCE RPC request.										
CVE-2013-3873	Microsoft IE contains a flaw that is triggered as user-supplied input is not properly sanitized. The issue occurs during the handling of HtmlLayout::SmartObject objects. Through manipulation of a document element, an attacker can cause a dangling pointer to be re-used after being freed. This may allow a context-dependent attacker to corrupt memory and cause a denial of service or potentially execute arbitrary code.										
CVE-2013-3785	Oracle PeopleSoft Enterprise HRMS contains an unspecified flaw in the Career's Home subcomponent that may allow a remote authenticated attacker to gain access to potentially sensitive information. No further details have been provided by the vendor.										
CVE-2012-1885	Heap-based buffer overflow in Microsoft Excel 2003 SP3, 2007 SP2 and SP3, and 2010 SP1; Office 2008 and 2011 for Mac; and Office Compatibility Pack SP2 and SP3 allows remote attackers to execute arbitrary code via a crafted spreadsheet, aka "Excel SerAuxErrBar Heap Overflow Vulnerability."										