



CVE-2011-1225

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2011-1225
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-04-13 20:26:00 UTC
Updated	2023-12-07 18:38:00 UTC
Description	win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, and Windows 7 SP1 and SP2 is susceptible to a buffer overflow attack. An attacker who successfully exploits this vulnerability could cause the system to crash or execute arbitrary code. This vulnerability is present in the following products: Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, and Windows 7 SP1 and SP2.

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows 2003 Server	All	sp2	All	All
Operating System	Microsoft	Windows 2003 Server	All	sp2	All	All
Operating System	Microsoft	Windows 7	-	All	All	All
Operating System	Microsoft	Windows 7	-	sp1	x64	All
Operating System	Microsoft	Windows 7	-	sp1	x86	All
Operating System	Microsoft	Windows 7	-	All	All	All
Operating System	Microsoft	Windows 7	-	sp1	x64	All
Operating System	Microsoft	Windows 7	-	sp1	x86	All
Operating System	Microsoft	Windows Server 2003	All	sp2	All	All
Operating System	Microsoft	Windows Server 2003	All	sp2	All	All
Operating System	Microsoft	Windows Server 2008	All	All	itanium	All
Operating System	Microsoft	Windows Server 2008	All	All	x32	All
Operating System	Microsoft	Windows Server 2008	All	All	x64	All
Operating System	Microsoft	Windows Server 2008	All	sp2	x32	All
Operating System	Microsoft	Windows Server 2008	All	sp2	x64	All
Operating System	Microsoft	Windows Server 2008	-	sp2	itanium	All
Operating System	Microsoft	Windows Server 2008	r2	All	itanium	All

Operating System	Microsoft	Windows Server 2008	r2	All	x64	All
Operating System	Microsoft	Windows Server 2008	All	All	itanium	All
Operating System	Microsoft	Windows Server 2008	All	All	x32	All
Operating System	Microsoft	Windows Server 2008	All	All	x64	All
Operating System	Microsoft	Windows Server 2008	All	sp2	x32	All
Operating System	Microsoft	Windows Server 2008	All	sp2	x64	All
Operating System	Microsoft	Windows Server 2008	-	sp2	itanium	All
Operating System	Microsoft	Windows Server 2008	r2	All	itanium	All
Operating System	Microsoft	Windows Server 2008	r2	All	x64	All
Operating System	Microsoft	Windows Vista	All	sp1	All	All
Operating System	Microsoft	Windows Vista	All	sp1	x64	All
Operating System	Microsoft	Windows Vista	All	sp2	All	All
Operating System	Microsoft	Windows Vista	All	sp2	x64	All
Operating System	Microsoft	Windows Vista	All	sp1	All	All
Operating System	Microsoft	Windows Vista	All	sp1	x64	All
Operating System	Microsoft	Windows Vista	All	sp2	All	All
Operating System	Microsoft	Windows Vista	All	sp2	x64	All
Operating System	Microsoft	Windows Xp	All	sp3	All	All
Operating System	Microsoft	Windows Xp	-	sp2	x64	All
Operating System	Microsoft	Windows Xp	All	sp3	All	All
Operating System	Microsoft	Windows Xp	-	sp2	x64	All

References

Reference	Source
Microsoft Security Bulletin MS11-034 - Important Microsoft Docs	MS
Microsoft Windows win32k.sys Driver Privilege Escalation Vulnerabilities - Secunia.com	SECUNIA
Microsoft Windows Kernel 'Win32k.sys' (CVE-2011-1225) Local Privilege Escalation Vulnerability	BID
ASA-2011-110 MS11-034 (2506223)	CONFIRM
Windows Kernel win32k.sys Lets Local Users Gain Elevated Privileges - SecurityTracker	SECTrack
US-CERT Technical Cyber Security Alert TA11-102A -- Microsoft Updates for Multiple Vulnerabilities	CERT
IBM X-Force Exchange	XF
MS11-034: Addressing vulnerabilities in the win32k subsystem - Security Research & Defense - Site Home - TechNet Blogs	MISC
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
Repository / Oval Repository	OVAL
CVE Program record	CVE.ORG
MSRC Security Updates	MSRC

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)