



CVE-2011-2011

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

Summary

CVE	CVE-2011-2011
State	PUBLISHED
Assigner	microsoft
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-10-12 02:52:44 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Serv

Risk And Classification

Primary CVSS: v2.0 7.2 from nvd@nist.gov

AV:L/AC:L/Au:N/C:C/I:C/A:C

Problem Types: CWE-399 | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:L/AC:L/Au:N/C:C/I:C/A:C

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 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 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	sp2	All	All
Operating System	Microsoft	Windows Xp	All	sp3	All	All
Operating System	Microsoft	Windows Xp	-	sp2	x64	All

Vendor Declared Affected Products					
Source	Vendor	Product	Version	Platforms	
CNA	Na	N/a	affected n/a	Not specified	

References
Reference
Repository / Oval Repository
SecurityTracker: Windows Kernel-Mode Drivers Memory Corruption Errors Let Remote Users Execute Arbitrary Code and Local Users Deny S
Microsoft Windows Kernel 'Win32k.sys' (CVE-2011-2011) Local Privilege Escalation Vulnerability
Microsoft Security Bulletin MS11-077 - Important Microsoft Docs
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.
There are currently no legacy QID mappings associated with this CVE.

