



CVE-2011-0676

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

Summary

CVE	CVE-2011-0676
State	PUBLISHED
Assigner	microsoft
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-04-13 20:26:24 UTC
Updated	2026-04-29 01:13:23 UTC
Description	win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from ADP

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Problem Types: NVD-CWE-Other | CWE-476 | n/a | CWE-476 CWE-476 NULL Pointer Dereference

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	7.2		AV:L/AC:L/Au:N/C:I/I:C/A:C

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

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	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	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						Source
ASA-2011-110 MS11-034 (2506223)						af854a3a-2127
US-CERT Technical Cyber Security Alert TA11-102A -- Microsoft Updates for Multiple Vulnerabilities						af854a3a-2127
MS11-034: Addressing vulnerabilities in the win32k subsystem - Security Research & Defense - Site Home - TechNet Blogs						af854a3a-2127
Microsoft Security Bulletin MS11-034 - Important Microsoft Docs						af854a3a-2127
Microsoft Windows win32k.sys Driver Privilege Escalation Vulnerabilities - Secunia.com						af854a3a-2127
Repository / Oval Repository						af854a3a-2127
IBM X-Force Exchange						af854a3a-2127
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH						af854a3a-2127
Repository / Oval Repository						af854a3a-2127
Windows Kernel win32k.sys Lets Local Users Gain Elevated Privileges - SecurityTracker						af854a3a-2127
Microsoft Windows Kernel 'Win32k.sys' (CVE-2011-0676) Local Privilege Escalation Vulnerability						af854a3a-2127
CVE Program record						CVE.ORG
NVD vulnerability detail						NVD
No vendor comments have been submitted for this CVE.						
There are currently no legacy QID mappings associated with this CVE.						