CVE-2014-4113

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

Summary

CVE	CVE-2014-4113
State	PUBLISHED
Assigner	microsoft
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-10-15 10:55:07 UTC
Updated	2026-04-22 16:49:05 UTC
Description	win32k.sys in the kernel-mode drivers in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from ADP

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

EPSS: 0.826610000 probability, percentile 0.992490000 (date 2026-05-10)

CISA KEV: Listed on 2022-05-04; due 2022-05-25; ransomware use Unknown

Problem Types: NVD-CWE-noinfo | n/a | CWE-noinfo Not enough information

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/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:N/UI:R/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	7.2		AV:L/AC:L/Au:N/C:C/I:C/A:C

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:N/UI:R/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

CISA Known Exploited Vulnerability

Vendor	Microsoft
Product	Win32k
Name	Microsoft Win32k Privilege Escalation Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2014-4113

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows 7	-	sp1	All	All
Operating System	Microsoft	Windows 8	-	All	All	All
Operating System	Microsoft	Windows 8.1	-	All	All	All
Operating System	Microsoft	Windows Rt	-	All	All	All
Operating System	Microsoft	Windows Rt 8.1	-	All	All	All
Operating System	Microsoft	Windows Server 2003	-	sp2	All	All
Operating System	Microsoft	Windows Server 2008	-	sp2	All	All

Operating System	Microsoft	Windows Server 2008	r2	sp1	All	All
Operating System	Microsoft	Windows Server 2012	-	All	All	All
Operating System	Microsoft	Windows Server 2012	r2	All	All	All
Operating System	Microsoft	Windows Vista	-	sp2	All	All

Vendor Declared Affected Products

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

References

Reference	Source
osvdb.org/show/osvdb/113167	af854a3a-2127-422b-9
Windows 8.0 - 8.1 x64 - TrackPopupMenu Privilege Escalation MS14-058 - Exploits Database	af854a3a-2127-422b-9
Microsoft Windows Kernel 'Win32k.sys' CVE-2014-4113 Local Privilege Escalation Vulnerability	af854a3a-2127-422b-9
Microsoft Security Bulletin MS14-058 - Critical | Microsoft Docs	af854a3a-2127-422b-9
About Secunia Research | Flexera	af854a3a-2127-422b-9
www.cisa.gov/known-exploited-vulnerabilities-catalog	134c704f-9b21-4f2e-91
Microsoft Windows Kernel - 'win32k.sys' Local Privilege Escalation (MS14-058) - Windows local Exploit	af854a3a-2127-422b-9
An Analysis of A Windows Kernel-Mode Vulnerability (CVE-2014-4113) | Security Intelligence Blog | Trend Micro	af854a3a-2127-422b-9
GitHub - sam-b/CVE-2014-4113: Trigger and exploit code for CVE-2014-4113	af854a3a-2127-422b-9
Windows TrackPopupMenu Win32k NULL Pointer Dereference	af854a3a-2127-422b-9
Windows 8.0 / 8.1 x64 TrackPopupMenu Privilege Escalation ≈ Packet Storm	af854a3a-2127-422b-9
Assessing Risk for the October 2014 Security Updates - Security Research & Defense - Site Home - TechNet Blogs	af854a3a-2127-422b-9
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD
CISA Known Exploited Vulnerabilities catalog	CISA

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
ADP	2022-05-04T00:00:00.000Z	CVE-2014-4113 added to CISA KEV

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