CVE-2015-2546

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

Summary

CVE	CVE-2015-2546
State	PUBLISHED
Assigner	microsoft
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-09-09 00:59:53 UTC
Updated	2026-04-22 16:16:40 UTC
Description	The kernel-mode driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Window

Risk And Classification

Primary CVSS: v3.1 8.2 HIGH from ADP

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

EPSS: 0.434650000 probability, percentile 0.975210000 (date 2026-04-24)

CISA KEV: Listed on 2022-03-15; due 2022-04-05; ransomware use Known

Problem Types: CWE-119 | n/a | CWE-119 CWE-119 Improper Restriction of Operations within the Bounds of a Memory Buffer

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	8.2	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	8.2	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	6.9		AV:L/AC:M/Au:N/C:C/I:C/A:C

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

Required

Scope

Changed

Confidentiality

High

Integrity

High

Availability

High

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

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Medium

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

CISA Known Exploited Vulnerability

Vendor	Microsoft
Product	Win32k
Name	Microsoft Win32k Memory Corruption Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2015-2546

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows 10 1507	-	All	All	All
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 2008	-	sp2	All	All
Operating System	Microsoft	Windows Server 2008	r2	sp1	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
Microsoft Security Bulletin MS15-097 - Critical | Microsoft Docs
Microsoft Graphics Component Bugs Let Remote Users Execute Arbitrary Code and Local Users Gain Elevated Privileges - SecurityTracker
www.cisa.gov/known-exploited-vulnerabilities-catalog
Microsoft Windows Kernel Mode Driver CVE-2015-2546 Local Privilege Escalation Vulnerability
CVE Program record
NVD vulnerability detail
CISA Known Exploited Vulnerabilities catalog

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
ADP	2022-03-15T00:00:00.000Z	CVE-2015-2546 added to CISA KEV

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