



# CVE-2015-2360

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2015-2360
<b>State</b>	PUBLISHED
<b>Assigner</b>	microsoft
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2015-06-10 01:59:38 UTC
<b>Updated</b>	2026-04-22 16:43:23 UTC
<b>Description</b>	win32k.sys in the kernel-mode drivers in Microsoft Windows Server 2003 SP2 and R2 SP2, Windows Vista SP2, Windows 9

## Risk And Classification

**Primary CVSS:** v3.1 8.8 HIGH from ADP

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

**EPSS:** 0.116010000 probability, percentile 0.936830000 (date 2026-04-22)

**CISA KEV:** Listed on 2022-05-25; due 2022-06-15; ransomware use Unknown

**Problem Types:** CWE-119 | CWE-416 | n/a | CWE-416 CWE-416 Use After Free

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	8.8	HIGH	CVSS:3.1/AV:N/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:C/I:C/A:C

## CVSS v3.1 Breakdown

Attack Vector

**Network**

Attack Complexity

**Low**

Privileges Required

**Low**

User Interaction

**None**

Scope

**Unchanged**

Confidentiality

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/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

### CISA Known Exploited Vulnerability

<b>Vendor</b>	Microsoft
<b>Product</b>	Win32k
<b>Name</b>	Microsoft Win32k Privilege Escalation Vulnerability
<b>Required Action</b>	Apply updates per vendor instructions.
<b>Notes</b>	<a href="https://nvd.nist.gov/vuln/detail/CVE-2015-2360">https://nvd.nist.gov/vuln/detail/CVE-2015-2360</a>

### 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 2003	r2	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 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
Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2360 Local Privilege Escalation Vulnerability	af854a3a-2127-4
www.cisa.gov/known-exploited-vulnerabilities-catalog	134c704f-9b21-4
Microsoft Security Bulletin MS15-061 - Important   Microsoft Docs	af854a3a-2127-4
Windows Kernel Lets Local Users Obtain Potentially Sensitive Information and Gain Elevated Privileges - SecurityTracker	af854a3a-2127-4
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	2022-05-25T00:00:00.000Z	CVE-2015-2360 added to CISA KEV

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](#)