CVE-2017-0263

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

Summary

CVE	CVE-2017-0263
State	PUBLISHED
Assigner	microsoft
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-05-12 14:29:05 UTC
Updated	2026-04-22 13:47:41 UTC
Description	The kernel-mode drivers in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Ser

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from nvd@nist.gov

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

EPSS: 0.184700000 probability, percentile 0.952530000 (date 2026-04-21)

CISA KEV: Listed on 2022-02-10; due 2022-08-10; ransomware use Unknown

Problem Types: CWE-416 | Elevation of Privilege | CWE-416 CWE-416 Use After Free

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

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-2017-0263

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 10 1511	-	All	All	All
Operating System	Microsoft	Windows 10 1607	-	All	All	All
Operating System	Microsoft	Windows 10 1703	-	All	All	All
Operating System	Microsoft	Windows 7	-	sp1	All	All
Operating System	Microsoft	Windows 8.1	-	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 2012	-	All	All	All
Operating System	Microsoft	Windows Server 2012	r2	All	All	All
Operating System	Microsoft	Windows Server 2016	-	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Microsoft Corporation	Microsoft Windows	affected Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows

References

Reference	Source
www.cisa.gov/known-exploited-vulnerabilities-catalog	134c704f-9b21-
FROM ANALYZING CVE-2017-0263 TO INVESTIGATING MENU MANAGEMENT COMPONENT - 小刀志	af854a3a-2127-
Windows Kernel 'win32k.sys' Bugs Let Local Users Deny Service and Gain Elevated Privileges - SecurityTracker	af854a3a-2127-
Microsoft Windows Kernel 'Win32k.sys' CVE-2017-0263 Local Privilege Escalation Vulnerability	af854a3a-2127-
portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0263	af854a3a-2127-
Microsoft Windows Manager (7 x86) - Menu Management Component UAF Privilege Elevation - Windows_x86 local Exploit	af854a3a-2127-
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	2022-02-10T00:00:00.000Z	CVE-2017-0263 added to CISA KEV

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

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