



CVE-2016-0175

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

Summary

CVE	CVE-2016-0175
State	PUBLISHED
Assigner	microsoft
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-05-11 01:59:15 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windo

Risk And Classification

Primary CVSS: v3.0 3.3 LOW from nvd@nist.gov

CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N

Problem Types: CWE-200 | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	3.3	LOW	CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N
2.0	nvd@nist.gov	Primary	2.1		AV:L/AC:L/Au:N/C:P/I:N/A:N

CVSS v3.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

None

Availability

None

CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows 10	All	All	All	All
Operating System	Microsoft	Windows 10	1511	All	All	All
Operating System	Microsoft	Windows 7	All	sp1	All	All
Operating System	Microsoft	Windows 7	-	sp1	x64	All
Operating System	Microsoft	Windows 8.1	All	All	All	All
Operating System	Microsoft	Windows Rt 8.1	All	All	All	All
Operating System	Microsoft	Windows Server 2008	All	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	All	sp2	All	All

Vendor Declared Affected Products

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

References

Reference	Source
-----------	--------

Windows Kernel-Mode Drivers Let Local Users Bypass ASLR and Gain Elevated Privileges - SecurityTracker	af854a3a-2127-422b-91ae-36
Microsoft Windows Kernel CVE-2016-0175 Local Security Bypass Vulnerability	af854a3a-2127-422b-91ae-36
Zero Day Initiative	af854a3a-2127-422b-91ae-36
Microsoft Security Bulletin MS16-062 - Important Microsoft Docs	af854a3a-2127-422b-91ae-36
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.

© [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](#)