



Microsoft Word Information Disclosure Vulnerability

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2026-40421
State	PUBLISHED
Assigner	microsoft
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-12 18:17:20 UTC
Updated	2026-05-12 18:17:20 UTC
Description	External control of file name or path in Microsoft Office Word allows an unauthorized attacker to disclose information over a

Risk And Classification

Primary CVSS: v3.1 4.3 MEDIUM from secure@microsoft.com

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

Problem Types: CWE-73 | CWE-73 CWE-73: External Control of File Name or Path

Version	Source	Type	Score	Severity	Vector
3.1	secure@microsoft.com	Primary	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N
3.1	CNA	CVSS	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:U/RL:O/RC:C

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

Low

Integrity

None

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Microsoft	Microsoft 365 Apps For Enterprise	affected 16.0.1 https://aka.ms/OfficeSecurityReleases custom	32-bit Systems, x6
CNA	Microsoft	Microsoft Office 2019	affected 19.0.0 https://aka.ms/OfficeSecurityReleases custom	32-bit Systems, x6
CNA	Microsoft	Microsoft Office LTSC 2021	affected 16.0.1 https://aka.ms/OfficeSecurityReleases custom	32-bit Systems, x6
CNA	Microsoft	Microsoft Office LTSC 2024	affected 16.0.0 https://aka.ms/OfficeSecurityReleases custom	32-bit Systems, x6
CNA	Microsoft	Microsoft Word 2016	affected 16.0.1 16.0.5552.1000 custom	32-bit Systems, x6

References

Reference	Source	Link	Tags
msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40421	secure@microsoft.com	msrc.microsoft.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

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