Microsoft Office Click-To-Run Elevation of Privilege Vulnerability

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

Summary

CVE	CVE-2026-40420
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	Improper access control in Microsoft Office Click-To-Run allows an authorized attacker to elevate privileges locally.

Risk And Classification

Primary CVSS: v3.1 8.8 HIGH from secure@microsoft.com

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

Problem Types: CWE-284 | CWE-284 CWE-284: Improper Access Control

Version	Source	Type	Score	Severity	Vector
3.1	secure@microsoft.com	Primary	8.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
3.1	CNA	CVSS	8.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C

CVSS v3.1 Breakdown

Attack Vector
Local

Attack Complexity
Low

Privileges Required
Low

User Interaction
None

Scope
Changed

Confidentiality
High

Integrity
High

Availability

High

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

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

References

Reference	Source	Link	Tags
msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40420	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.