Microsoft Defender Elevation of Privilege Vulnerability

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

Summary

CVE	CVE-2026-33825
State	PUBLISHED
Assigner	microsoft
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-14 18:17:35 UTC
Updated	2026-04-23 17:26:30 UTC
Description	Insufficient granularity of access control in Microsoft Defender allows an authorized attacker to elevate privileges locally.

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from secure@microsoft.com

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

EPSS: 0.038180000 probability, percentile 0.881450000 (date 2026-04-24)

CISA KEV: Listed on 2026-04-22; due 2026-05-06; ransomware use Unknown

Problem Types: CWE-1220 | CWE-1220 CWE-1220: Insufficient Granularity of Access Control

Version	Source	Type	Score	Severity	Vector
3.1	secure@microsoft.com	Secondary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

High

ntegrity

High

Availability

High

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

CISA Known Exploited Vulnerability

Vendor	Microsoft
Product	Defender
Name	Microsoft Defender Insufficient Granularity of Access Control Vulnerability
Required Action	Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.
Notes	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33825 ; https://nvd.nist.gov/vuln/detail/CVE-2026-33825

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Defender Antimalware Platform	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Microsoft	Microsoft Defender Antimalware Platform	affected 4.0.0.0 4.18.26030.3011 custom	Not specified

References

Reference	Source	Link	Tags
www.cisa.gov/known-exploited-vulnerabilities-catalog	134c704f-9b21-4f2e-91b3-4a467353bcc0	www.cisa.gov	US Gove
www.huntress.com/blog/nightmare-eclipse-intrusion	134c704f-9b21-4f2e-91b3-4a467353bcc0	www.huntress.com	Third Pa
msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33825	secure@microsoft.com	msrc.microsoft.com	Vendor A
CVE Program record	CVE.ORG	www.cve.org	canonica
NVD vulnerability detail	NVD	nvd.nist.gov	canonica
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov	kev

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**