Endpoint DLP Driver Out-of-Bounds Read

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

Summary

CVE	CVE-2026-2810
State	PUBLISHED
Assigner	Netskope
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-29 16:16:22 UTC
Updated	2026-04-30 15:13:14 UTC
Description	Netskope was notified about a potential gap in the Endpoint DLP Module for Netskope Client on Windows systems. The su

Risk And Classification

Primary CVSS: v4.0 6.8 MEDIUM from psirt@netskope.com

CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:H/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000160000 probability, percentile 0.036000000 (date 2026-05-05)

Problem Types: CWE-125 | CWE-125 CWE-125 Out-of-bounds read

Version	Source	Type	Score	Severity	Vector
4.0	psirt@netskope.com	Secondary	6.8	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:H/E:X/
4.0	CNA	CVSS	6.8	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:H

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

Low

User Interaction

None

Confidentiality

None

ntegrity

None

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

High

CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:H/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Netskope	Client	affected 129.1.8,132.0.23,135.1.0,136.1 custom	Windows

References

Reference	Source	Link
www.netskope.com/resources/netskope-resources/netskope-security-advisory-nskps...	psirt@netskope.com	www.netskope.com
support.netskope.com/s/article/Netskope-Security-Advisory-NSKPSA-2026-002-Netskope...	psirt@netskope.com	support.netskope.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Tom Brice (en)

Additional Advisory Data

Workarounds

CNA: There are no direct workarounds. Some AV and EDR solutions may be able to detect behaviors associated with exploiting this vulnerability.

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