



# Endpoint DLP Driver Out-of-Bounds Read

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2026-2810
<b>State</b>	PUBLISHED
<b>Assigner</b>	Netskope
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-29 16:16:22 UTC
<b>Updated</b>	2026-04-30 15:13:14 UTC
<b>Description</b>	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/MSX/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

Integrity

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/MSX: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	<a href="#">Netskope</a>	Client	affected 129.1.8,132.0.23,135.1.0,136.1 custom	Windows

### References

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

### 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.

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](#)