Netskope Security Advisory

Security Advisory (Public Disclosure)

Netskope Security Advisory – Netskope Client is impacted by Heap Overflow vulnerability

Security Advisory ID:	NSKPSA-2025-003	Severity Rating:	Medium
First Published:	Aug 13, 2025	Overall CVSS Score:	5.7
Version:	1.0	CVE-ID:	CVE-2025-5942

Description

Netskope is notified about a potential gap in its agent (NS Client) on Windows systems in which an unprivileged user can potentially trigger a heap overflow in the epdlpdrv.sys driver, leading to a Blue-Screen-of-Death (BSOD). Success exploitation could also be performed by an unprivileged user whose NS Client is configured to use Netskope Endpoint DLP. A successful exploit could result in a denial-of-service for the local machine.

Affected Product(s) and Version(s)

Product Name: Netskope Client + Endpoint DLP
Affected Platform: Windows
Affected Versions: All versions below R129

CVE-ID(s)

CVE-2025-5942

Remediation

Netskope has released a security patch for the issue. Please see below

- Patch versions: R129 and above

Netskope Security Advisory

- Patch backported versions: R126.0.9 and above

Netskope download Instructions - Download Netskope Client and Scripts – Netskope Support

Workaround

There are no workarounds available at this time.

General Security Best Practices

Netskope recommends using security hardening options available in the product and configuring them to harden the security of a Netskope tenant- https://docs.netskope.com/en/secure-tenant-configuration-and-hardening/

Special Notes and Acknowledgement

Netskope credits Thomas Brice for reporting this flaw.

Exploitation and Public Disclosures

Netskope is not aware of any active exploitation of the security issue.

Revision History

Version	Date	Section	Notes
1.0	13 Aug 2025		Initial Release

Legal Disclaimer:

To the maximum extent permitted by applicable law, information provided in this notice is provided "as is" without warranty of any kind. Your use of the information in this notice or materials linked herein are at your own risk. This notice and all aspects of Netskope's Product Security Incident Response Policy are subject to change without notice. Response is not guaranteed for any specific issue or class of issues. Your entitlements regarding warranties, support and maintenance, including vulnerabilities in any Netskope software or service, are governed solely by the applicable master agreement between Netskope and you. The statements in this notice do not modify, enlarge or otherwise amend any of your rights under the applicable master agreement, or create any additional warranties or commitments.

About Netskope

Netskope, a leader in modern security and networking, addresses the needs of both security and networking teams by providing optimized access and real-time, context-based security for people, devices, and data anywhere they go. Thousands of customers, including more than 30 of the Fortune 100, trust the Netskope One platform, its Zero Trust Engine, and its powerful NewEdge network to reduce risk and gain full visibility and control over cloud, AI, SaaS, web, and private applications—providing security and accelerating performance without trade-offs.