Netskope Security Advisory

Security Advisory (Public Disclosure)

Netskope Security Advisory – Endpoint DLP Driver Improper Service Loading Vulnerability

---

Security Advisory ID:	NSKPSA-2025-005	Severity Rating:	Medium
First Published:	Nov 25, 2025	Overall CVSS Score:	5.9
Version:	1.0	CVE-ID:	CVE-2025-11156

Description

Netskope was notified of a vulnerability within its Netskope Client Endpoint DLP driver (epdlpdrv.sys) on Windows systems. The vulnerability potentially allows a local, authenticated user with administrator privileges to improperly load the driver as a generic kernel service, which triggers a null-pointer dereference and causes a system crash (Blue-Screen-of-Death). A successful exploit may result in a denial-of-service for the affected machine.

Affected Product(s) and Version(s)

- Product Name: Netskope Client + Endpoint DLP
- Affected Platform: Windows
- Affected Versions: All versions prior to R132

CVE-ID(s)

- CVE-2025-11156

Remediation

Netskope Security Advisory

Netskope has patched the issue and released a new version R132. Customers are recommended to update the Netskope Client version on end-user machines to R132 or above. Customers utilizing the Fail-Safe feature must update to R132.0.7 or later (refer to Netskope Service Client Fail-Close Failure for details).

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

Workaround

Customers can block any process attempting to create a kernel service pointing to epdlpdrv.sys .

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://support.netskope.com/s/article/Secure-Tenant-Configuration

Special Notes and Acknowledgement

Netskope credits Ahmad Abdillah bin Zaini at Cybersecurity Agency of Singapore 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	Nov 25, 2025		Initial Release

Legal Disclaimer:

Netskope Security Advisory

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.