Netskope Security Advisory

Endpoint DLP double-fetch leading to heap-overflow

Security Advisory ID:	NSKPSA-2024-003	Severity Rating:	Medium
First Published:	Dec 19, 2024	Overall CVSS Score:	5.6
Version:	1.0	CVE-ID:	CVE-2024-11616

Description

Netskope was made aware of a security vulnerability in Netskope Endpoint DLP's Content Control Driver where a double-fetch issue leads to heap overflow. The vulnerability arises from the fact that the **NumberOfBytes** argument to **ExAllocatePoolWithTag**, and the **Length** argument for **RtlCopyMemory**, both independently dereference their value from the user supplied input buffer inside the **EpdlpSetUsbAction** function, known as a double-fetch. If this length value grows to a higher value in between these two calls, it will result in the **RtlCopyMemory** call copying user-supplied memory contents outside the range of the allocated buffer, resulting in a heap overflow. A malicious attacker will need admin privileges to exploit the issue.

Affected Product(s) and Version(s)

Product name: Netskope Endpoint DLP
Affected Platform: Windows
Affected Versions: All version below R119

CVE-ID(s)

CVE-2024-11616
CVSS4.0/AV:L/AC:H/AT:P/PR:H/UI:N/VC:N/VI:N/VA:H/SC:N/SI:L/SA:N (5.6)

Netskope Security Advisory

Remediation

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

- Patch versions: R119 and above
- Patch backported versions: R114 and R117

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

Workaround

Enabling tamperproofing using "Protect Netskope Client Configuration and Resources" will prevent the execution of the vulnerability.
Here is the guide to enable the configurations - https://docs.netskope.com/en/secure-tenant-configuration-and-hardening/#protection-of-client-resources-post-enrollment-1

General Security Best Practices

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

Special Notes and Acknowledgement

Netskope credits Thomas Brice from Oxford Nanopore Technologies 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	19 December 2024		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, the SASE leader, safely and quickly connects users directly to the internet, any application, and their infrastructure from any device, on or off the network. With CASB, SWG, and ZTNA built natively in a single platform, the Netskope Security Cloud provides the most granular context, via patented technology, to enable conditional access and user awareness while enforcing zero trust principles across data protection and threat prevention everywhere. Unlike others who force tradeoffs between security and networking, Netskope’s global security private cloud provides full compute capabilities at the edge.
Netskope is fast everywhere, data-centric, and cloud-smart, all while enabling good digital citizenship and providing a lower total-cost-of-ownership.