Netskope Security Advisory & Communication

Security Advisory - Public Disclosure

Netskope Security Advisory – Netskope Client configurations tampering with MITM

Security Advisory ID:	NSKPSA-2024-002	Severity Rating:	High
First Published:	Aug 13, 2025	Overall CVSS Score:	7.0
Version:	1.0	CVE-ID:	CVE-2024-7402

Description

Netskope was notified about a potential gap in its agent (Netskope Client) in which a malicious insider can tamper with the Netskope Client configuration by performing MITM (Man-in-the-Middle) attacks on the Netskope Client communication channel. **A successful exploitation would require administrative privileges on the machine**. A successful exploit can result in temporarily altering the configuration of Netskope Client or permanently disabling or removing the agent from the machine.

Affected Product(s) and Version(s)

- Product - Netskope Client
- Platform - All
- Versions - All (Unless the fix is enabled with supported versions)

CVE-ID(s)

CVE-2024-7402
Base Score: CVSS:4.0/AV:L/AC:L/AT:P/PR:H/UI:N/VC:N/VI:H/VA:N/SC:H/SI:H/SA:H

Remediation

Netskope has added a fix in Netskope Client R123(123.0.16), 126(126.0.9), R129 or higher with an option to enable the fix from tenant UI for administrators.
Netskope download Instructions - Download Netskope Client and Scripts – Netskope Support

Workaround

There are no workarounds to protect against the security issue apart from preventing users from installing MITM tools such as Burp and ZAP, or preventing users from installing any 3rd party certificates in Operating Systems trust stores.

General Security Best Practices

- Always keep software and applications updated with the latest versions
- Set up monitoring of applications to detect any abuses
- Configure and deploy the applications with hardening options as documented here - https://support.netskope.com/s/article/Secure-Tenant-Configuration

Special Notes and Acknowledgement

Netskope credits Sander de Wit for reporting this flaw.

Exploitation and Public Disclosures

Netskope is not aware of any active exploitation.

Revision History

Version	Date	Section	Notes
1.0	13 August, 2025		Initial

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

Netskope Security Advisory & Communication

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.