Netskope Security Advisory

Security Advisory (Public Disclosure)

Netskope Security Advisory – Netskope Client installer with symbolic link following vulnerability leading to privilege escalation

---

Security Advisory ID:	NSKPSA-2024-004	Severity Rating:	Medium
First Published:	Apr 15, 2025	Overall CVSS Score:	5.2
Version:	1.0	CVE-ID:	CVE-2024-13177

Description

Netskope Client on Mac OS is impacted by a vulnerability in which the postinstall script does not properly validate the path of the file “nsinstallation”. A standard user could potentially create a symlink of the file “nsinstallation” to escalate the privileges of a different file on the system.

Affected Product(s) and Version(s)

Product name: Netskope Client
Affected Platform: MacOS
Affected Versions: All versions below R123

CVE-ID(s)

CVE-2024-13177

CVSS:4.0/AV:L/AC:H/AT:N/PR:L/UI:N/VC:N/VI:N/VA:N/SC:H/SI:H/SA:H (5.2)

Netskope Security Advisory

Remediation

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

- Patch versions: R123 and above
- Patch backported versions: EHF Versions 117.1.11.2310 and 120.1.10.2306

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 - https://docs.netskope.com/en/secure-tenant-configuration-and-hardening/

Special Notes and Acknowledgement

Netskope credits Max Keasley of WithSecure Consulting 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	15 Apr 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, 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.