Title: Netskope Security Advisory – Local privilege escalation vulnerability in Netskope Client on macOS.

Security Advisory ID:	NSKPSA-2021-002
Version:	1.0
Status:	Published
Last Modified:	December 20, 2021

Who should read this document:	Technical and Security Personnel
Impact of Vulnerability:	Privilege Escalation
CVE Number:	CVE-2021-41388
Severity Rating:	High
Overall CVSS Score:	CVSS:3.1- 7.0 AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H
Recommendations:	Install or update to the latest version released r89.x & above
Security Advisory Replacement:	None
Caveats:	None
Affected Software:	Netskope Client on macOS v88 and earlier

Updated Software Version:	Netskope Release 89 and later
Special Notes and Acknowledgements:	Netskope would like to thank Red Team DART from The Home Depot for reporting the issue.
CWE Reference:	CWE - CWE-269: Improper Privilege Management (4.5) (mitre.org) CWE - CWE-250: Execution with Unnecessary Privileges (4.5) (mitre.org)
Exploit Code Maturity (E)	Proof-of-Concept (P)
Remediation Level (RL)	Official Fix (O)
Report Confidence (RC)	Confirmed (C)

Description;

Netskope client prior to 89.x on macOS is impacted by a local privilege escalation vulnerability. The XPC implementation of nsAuxiliarySvc process does not perform validation on new connections before accepting the connection. Thus any low privileged user can connect and call external methods defined in XPC service as root, elevating their privilege to the highest level.

Affected Components:

- Netskope Client v88.x and earlier on macOS

Remediation:

Netskope has patched the issue and released a new version of Netskope client.

Customers are advised to upgrade the software to the latest version (89 or above)

Netskope mac OS NSclient download Instructions can be found here - Download Netskope Client and Scripts – Netskope Support

Workaround:

No work around exists to mitigate the issue apart from upgrading to the latest version.

Special Notes and Acknowledgement:

Netskope would like to thank Red Team DART from The Home Depot for reporting this vulnerability.

Support:

Netskope Support Details can be obtained from here.

Frequently Asked Questions (FAQs):

1. **Do we use this for communication when a customer is abusing our systems?**

   No, please reachout to psirt@netskope.com for support on this.

2. **What is affected by this security vulnerability?**

   Netskope Client v88.x and earlier on macOS.

3. **Do I need to Update Immediately?**

If yes: Netskope recommends that all customers run the latest version of software and evaluate this notification with other existing controls to make a determination. Netskope also recommends that customers leverage the CVSS v3.1 extended scoring or OWASP vulnerability criticality scoring tools to support his decision.

4. **Affected Versions:**
    - 88.x and earlier
5. **Protected Versions:**
    - 89.x and later

Netskope recommends that all customers verify that they have applied the latest updates.

6. **What issues do this Release/ patch address?**
    - The detailed changelog of the release can be obtained from here
7. **How do I know if my Netskope Client on macOS is vulnerable or not?**

To check the Netskope Client version on macOS, navigate to Netskope Client and then Right Click to see the option list. From the list select ‘About’, a pop up screen will display the used version.

8. **What has Netskope done to resolve the issue?**

Netskope has released a new version of the software to address this security flaw..

9. **Where do I download the fix?**

Please visit the release notes on https://support.netskope.com

10. **How does Netskope respond to this and any other security flaws**

Netskope has a robust Cybersecurity program to address all security flaws in its products reported by external entities and found by internal assessment. The details of Netskope security program is listed here - Security, Compliance and Assurance (netskope.com)

11. **How do I find out about security vulnerabilities with your products?**

    https://www.netskope.com/company/security-compliance-and-assurance/security-advisories-and-disclosures

12. **How was this found?**

    This issue was reported by Red Team DART from The Home Depot.

Resources:

Support Website: **https://www.netskope.com/services#support**

Contacts: support@netskope.com , PSIRT@netskope.com