Netskope Security Advisory & Communication

Netskope Security Advisory – Local privilege escalation using log files in Netskope Client

---

Security Advisory ID:	NSKPSA-2023-002	Severity Rating:	High
First Published:	May 10, 2023	Overall CVSS Score:	7.0
Version:	1.0		

Description

The Netskope client service on Windows runs as NT AUTHORITY\SYSTEM which writes log files to a writable directory (C:\Users\Public\netSkope) for a standard user. The files are created and written with a SYSTEM account except one file (logplaceholder) which inherits permission giving all users full access control list. Netskope client restricts access to this file by allowing only read permissions as a standard user. Whenever the Netskope client service restarts, it deletes the logplaceholder and recreates, creating a race condition, which can be exploited by a malicious local user to create the file and set ACL permissions on the file. Once the file is created by a malicious user with proper ACL permissions, all files within C:\Users\Public\netSkope\ becomes modifiable by the unprivileged user. By using Windows pseudo-symlink, these files can be pointed to other places in the system and thus malicious users will be able to elevate privileges.

Affected Product(s) and Version(s)

Netskope Client for Windows v95 & prior

CVE-ID(s)

CVE-2022-4149

Remediation

Netskope Security Advisory & Communication

Netskope has patched the vulnerability and released a binary with a fix. Customers are recommended to upgrade their Netskope clients to v100 or later
Netskope download Instructions - Download Netskope Client and Scripts – Netskope Support

Workaround

Netskope has provided a documented guide on hardening Netskope Client with additional security features which will further strengthen security of the product. Here are the guidelines - https://docs.netskope.com/en/netskope-client-hardening.html

General Security Best Practices

Following are the security best practices recommended for Netskope products:

- Always keep the Netskope products to the latest version
- Follow the Netskope hardening guides provided here - https://support.netskope.com/s/article/Secure-Tenant-Configuration
- Deploy applications by following least privilege principle
- Purge all data, associated files from end machine after remove the application

Special Notes and Acknowledgement

Netskope credits Dawson Medin from Mandiant for reporting this flaw.

Exploitation and Public Disclosures

Netskope is not aware of any public disclosure and exploitation of this vulnerability at the time of publication.

Revision History

Version	Date	Section	Notes
1.0	May 10, 2023		Initial Release

Legal Disclaimer:

Netskope Security Advisory & Communication

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.