



Netskope Security Advisory & Communication

Netskope Security Advisory – Local privilege escalation vulnerability in Netskope Client

Security Advisory ID: NSKPSA-2023-001 Severity Rating: **High**

First Published: **May 10, 2023** Overall CVSS Score: 7.0

Version: 1.0

Description

The Netskope client service running with NT\SYSTEM privileges accepts network connections from localhost to start various services and execute commands. The connection handling function in this service utilized a relative path to download and unzip configuration files on the machine. This relative path provided a way for local users to write arbitrary files at a location which is accessible to only higher privileged users. This can be exploited by local users to execute code with NT\SYSTEM privileges on the end machine.

Affected Product(s) and Version(s)

- Netskope Client for Windows v99 & Prior

CVE-ID(s)

- CVE-2023-2270

Remediation

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](#)



Netskope Security Advisory & Communication

Workaround

Netskope has provided a documented guide on hardening Netskope Client with additional security features which will further the security of the product. Here are the guidelines - <https://docs.netskope.com/en/netkope-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 Jean-Jamil Khalife from HDWSec 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

<u>Version</u>	<u>Date</u>	<u>Section</u>	<u>Notes</u>
1.0	May 10, 2023		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.



Netskope Security Advisory & Communication

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.