Netskope Security Advisory & Communication

Security Advisory

Netskope Security Advisory – Netskope NSClient is impacted by local privilege escalation vulnerability to terminate the NSClient

Security Advisory ID:	NSKPSA-2023-003	Severity Rating:	Medium
First Published:	Oct 4, 2023	Overall CVSS Score:	6.6
Version:	1.0	CVE-ID:	CVE-2023-4996

Description

Netskope was made aware of a security vulnerability in its NSClient product where a malicious non-admin user can disable the Netskope client by using a specially-crafted package. The root cause of the problem was a user control code when called by a Windows ServiceController did not validate the permissions associated with the user before executing the user control code. This user control code had permissions to terminate the NSClient service.

Affected Product(s) and Version(s)

Product - Netskope Client
Platform - Windows
Version - R100 & Prior

CVE-ID(s)

CVE-2023-4996

Remediation

Netskope patched the issue and released a new version. The issue was fixed in Release101. Customers are recommended to upgrade their client to the versions R101 or greater.
Netskope download Instructions - Download Netskope Client and Scripts – Netskope Support

Workaround

There are no workarounds available for this issue.

General Security Best Practices

Netskope recommends all our customers to keep their environments updated with latest version of the software and also enable and configure the secure hardening configurations available in the platform for the application: https://support.netskope.com/s/article/Secure-Tenant-Configuration

Special Notes and Acknowledgement

Netskope credits Alexander Katziv from Novartis for reporting this flaw.

Exploitation and Public Disclosures

Netskope is not aware of any public exploitations of the issue till the advisory is published

Revision History

Version	Date	Section	Notes
1.0	04/10/2023		Initial Notification

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

Netskope Security Advisory & Communication

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.