Netskope Security Advisory

Netskope Security Advisory – Netskope client enrollment bypass issue

Security Advisory ID:	NSKPSA-2024-001	Severity Rating:	High
First Communicated:	Apr 18, 2024	Overall CVSS Score:	8.5
Version:	1.0	CVE-ID:	CVE-2024-7401

Description

Netskope was notified about a security gap in Netskope Client enrollment process where NSClient is using a static token “Orgkey” as authentication parameter. Since this a static token, if leaked, cannot be rotated or revoked. A malicious actor can use this token to enroll NSClient from a customer’s tenant and impersonate.

Affected Product(s) and Version(s)

The gap is not associated with the NSClient package. Please refer the documentation - https://docs.netskope.com/en/secure-enrollment/

CVE-ID(s)

CVE-2024-7401

Remediation

Netskope has fixed the gap and recommends customers to review their deployments of Netskope Client and enable the fix in their tenants. Here is the detailed guide - https://docs.netskope.com/en/secure-enrollment/

Workaround

There is no countermeasure available to remediate the gap without enabling Secure Enrollment, but follow the below steps to minimize the risk:

Netskope Security Advisory

Enable device compliance and device classification
Create a policy to block all traffic for the devices which are not meeting the device compliance checks and are not falling under proper device classification.

General Security Best Practices

Netskope recommends reviewing the security guidelines and hardening options listed on the page https://support.netskope.com/s/article/Secure-Tenant-Configuration and using them to further harden the tenants.

Special Notes and Acknowledgement

Netskope credits Sander di Wit for reporting this flaw.

Exploitation and Public Disclosures

Netskope has received isolated reports of abuse of this known exploit by Bug Bounty hunters. Netskope is happy to help customers detect any abuse and help them contain and remediate the incident, if any.

Revision History

Version	Date	Section	Notes
1.0	26/08/2024		Initial

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

Netskope Security Advisory

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.