Netskope Security Advisory

Netskope Security Advisory – Sensitive information stored in logs for NSclient

---

Security Advisory ID: NSKPSA-2022-001   Severity Rating: High

First Communicated: Mar 21, 2022   Overall CVSS Score: 8.4

Version: 1.0

Description

Netskope client is impacted by a vulnerability where an authenticated, local attacker can view sensitive information stored in NSClient logs which should be restricted. The vulnerability exists because the sensitive information is not masked/scrubbed before writing in the logs. A malicious user can use the sensitive information to download data and impersonate another user.
CWE-532: Insertion of Sensitive Information into Log File

Affected Product(s) and Version(s)

Netskope Client vR91 and Prior

CVE-ID(s)

CVE-2021-44862

Remediation

Netskope has patched this vulnerability and released a new version. All customers are recommended to upgrade their NSClients to the latest version. To download latest version, please refer to download Instructions - [Download Netskope Client and Scripts – Netskope Support](#)

Netskope reference -
https://support.netskope.com/s/article/NSKPSA-2022-001-Netskope-Security-Advisory-Sensitive-information-in-audit-logs

Netskope Security Advisory

Workaround

There are no workarounds for this vulnerability other than upgrading to the latest version.

General Security Best Practices

Follow the secure tenant configurations to enhance the security of tenants which are listed here - https://support.netskope.com/s/article/Secure-Tenant-Configuration

Special Notes and Acknowledgement

Netskope credits Ben O'Dea and Josh Wilson from IAG Australia for reporting this

vulnerability.

Exploitation and Public Disclosures

Netskope is not aware of any public exploitation or disclosures before this date.

Revision History

Version	Date	Section	Notes
1.0	Mar 21, 2022		Initial Disclosure

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 the Netskope 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.

Netskope Security Advisory

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.