Release 78 Security Advisory - NSKPSA2020-001

Netskope Security Advisory – Fix for Privilege Escalation Vulnerability Discovered in Netskope Windows Client

Security Advisory ID: NSKPSA2020-001

Version: 1.0

Status: Published

Last Modified: September 23rd 2020

Who should read this document	Technical and Security Personnel
Impact of Vulnerability	Privilege Escalation
CVE Number	CVE-2020-24576 (reserved number)
Severity Rating	High
Overall CVSS Score	CVSS 7.3 (pre-fix release) CVSS 6.8 (post-fix release)
Recommendations	Update to the latest release of the client release.
Security Advisory Replacement	None
Caveats	None
Affected Software	Netskope Client R77 and prior releases
Updated Software Version	Release 78
Special Notes and Acknowledgements	The Home Depot - Red Team DART
CWE Reference	CWE-269: Improper Privilege Management

Description

Netskope takes the protection of our customers' information and the services we provide very seriously and endeavors to be responsible and transparent in the disclosure of any issues related to the Netskope product. Netskope is releasing this security advisory to provide information about a fix to a vulnerability discovered within the Netskope Windows Client. Without the fix to this vulnerability, an attacker could perform a privileged escalation attack. This advisory also provides guidance as to what security professionals who have yet to implement the fix can do to mitigate potential attacks that use the vulnerabilities; and what Netskope is doing as part of its ongoing investigation.

This Release/patch remediates the following issues: **CVE-2020-24576 (This is a reserved number. As such, details online will not be available until the CVE publishes)**

Affected Components

Netskope Windows Client Service (stAgentSvc.exe)

Remediation

Netskope Client Release 78. Download instructions can be found here.

Workaround

As of now, there is no workaround. Please evaluate updating to latest release of Netskope the Windows Client.

Special Notes and Acknowledgement

Netskope credits Red Team DART from The Home Depot for reporting this vulnerability.

This security Advisory was written by the Product Security Incident Response Team, Netskope, Inc.

FAQs

What is affected by this security vulnerability?

Netskope Windows Client R77 and earlier.

Do I need to Update Immediately?

Yes, Netskope recommends that all customers run the latest version of software and evaluate this notification with other existing controls to make a determination. Netskope also recommends that customers use the CVSS v3.1 extended scoring or OWASP vulnerability criticality scoring tools to support their decision.

Affected Versions

Any Netskope Client deployment on Windows before R78.

Protected Versions

R78 or later. Netskope recommends that all customers verify that they have applied the latest updates.

What issues does this release and/or patch address?

The release includes the fix for the reported issue as well as other items which can be found with in our release notes: Netskope Support Release Notes Link

How do I know if my Netskope Client is vulnerable or not?

The product and version can be found by navigating to the Netskope Client, Right Click and seeing “About”. An example is below:

What has Netskope done to resolve the issue?
Netskope has released a new release to address this security flaw.

Where do I download the fix?
Please visit the release notes on support.netskope.com.

How does Netskope respond to this and any other security flaws?
Netskope follows public guidance for reporting concerns and issues from the research community which can be found at: https://www.netskope.com/vulnerability-disclosure-policy. In addition, Netskope follows a documented triage, remediation, and testing process for any reported items.

How do I find out about security vulnerabilities with your products?
Please review the release notes and security advisories on support.netskope.com.

How was this found?
This was reported to Netskope from The Home Depot - Red Team DART.

What is a “golden release”?
A golden release is a release of our client that undergos extensive test coverage and support backward compatibility up to two previous versions. We recommend that you deploy the golden release of the Client to the endpoints when the auto-update is disabled. More information can be found on our support website.