

Seems like there is a more localized page available for your location.

United S... ▼

Continue




< Security Advisory

# Synology-SA-26:05 Synology SSL VPN Client

Publish Time: 2026-04-10 17:21:40 UTC+8

Last Updated: 2026-04-10 17:21:40 UTC+8

 Severity **Important**

 Status **Resolved**

## Abstract

Synology has released a security update for the Synology SSL VPN Client utility to address vulnerabilities:

sensitive files from  
TTP service when a  
r manipulate the PIN  
orized VPN

### We value your privacy

We use cookies to personalize your use of our site. This includes third-party cookies for that we use for advertising and site analytics. See our [Privacy Statement](#) and [Cookie Policy](#) for more information on how we collect and use data.

Cookie Options

Reject All

OK



Seems like there is a more localized page available for your location.



Please refer to the **Affected Products** table for the corresponding updates.

### Affected Products

Product	Severity	Fixed Release Availability
Synology SSL VPN Client	Important	Upgrade to 1.4.5-0684 or above.

### Mitigation

None

### Detail

- CVE-2021-47960
  - Severity: Important
  - CVSS3 Base Score: 6.5
  - CVSS3 Vector: [CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N](#)
  - [CWE-552: Files or Directories Accessible to External Parties](#)
  - A files or directories accessible to external parties vulnerability in Synology SSL VPN Client before 1.4.5-0684 allows remote attackers to access files within the installation directory via a local HTTP server bound to the loopback interface. By leveraging user interaction with a

es such as  
formation

#### We value your privacy

We use cookies to personalize your use of our site. This includes third-party cookies for that we use for advertising and site analytics. See our [Privacy Statement](#) and [Cookie Policy](#) for more information on how we collect and use data.

Cookie Options

Reject All

OK



Seems like there is a more localized page available for your location.



- [CVE-2026-0684: Plaintext Storage of a Password](#)
- A plaintext storage of a password vulnerability in Synology SSL VPN Client before 1.4.5-0684 allows remote attackers to access or influence the user's PIN code due to insecure storage. This may lead to unauthorized VPN configuration and potential interception of subsequent VPN traffic when combined with user interaction.

### Acknowledgement

Laurent Sibilla (<https://www.linkedin.com/in/lisibilla/>)

### Reference

- [CVE-2021-47960](#)
- [CVE-2021-47961](#)

### Revision

Revision	Date	Description
1	2026-04-10	Initial public release.
2	2026-04-10	Disclosed vulnerability details.

#### We value your privacy

We use cookies to personalize your use of our site. This includes third-party cookies for that we use for advertising and site analytics. See our [Privacy Statement](#) and [Cookie Policy](#) for more information on how we collect and use data.

Cookie Options

Reject All

OK



Seems like there is a more localized page available for your location.



Downloads



Newsletter

Company



Sales



Compatibility



Resources



Copyright © 2026 Synology Inc. All rights reserved. [Terms & Conditions](#) | [Privacy](#) | [Cookie Preference](#)

Global - English

### We value your privacy

We use cookies to personalize your use of our site. This includes third-party cookies for that we use for advertising and site analytics. See our [Privacy Statement](#) and [Cookie Policy](#) for more information on how we collect and use data.

Cookie Options

Reject All

OK

