



Product Advisory

Product Family:	StrideLinx Comm Products	Number:	PA-COM-010
Part Numbers:	SE-SLxxxx	Date Issued:	08/05/2026
Subject:	StrideLinx VPN Client Critical Security Patch	Revision:	Original

Purpose Fix a critical security vulnerability that would allow an attacker to perform remote code execution on the computer running the client with elevated privileges.

Affected Products Hardware: Stridelinx Cloud Service licenses with the following part numbers:

Part Number	Affected Versions
SE-SLxxxx	Any system using StrideLinx VPN client to access StrideLinx routers to create a VPN tunnel that currently has v1.4.6 and older.

Summary A critical vulnerability was identified and fixed in the StrideLinx VPN Client during internal security testing. The vulnerability would allow an attacker to perform remote code execution on the computer running the client with elevated privileges.
StrideLinx Cloud will no longer accept VPN clients that are not version 1.4.7 or later, preventing the vulnerability from being exploited.
There has been no indication that the vulnerability was exploited, and we are aware of no public disclosure or exploit for it.

Solution **Update StrideLinx VPN Client to v1.4.7 or later**

Update the StrideLinx VPN Client to v1.4.7 or later on every computer where it is installed. Since affected versions are no longer allowed to connect, updating is needed to restore remote access. Where the client is no longer needed, uninstalling it removes the affected software from that computer.

Full instructions for installing and uninstalling are in this [support article](#).

The client is installed per user, so it may be on computers that appear in no central overview. Include colleagues, contractors and service partners who use it on their own equipment.

Product Description The StrideLinx VPN Client is a lightweight application that runs in the background of the computer as a service or daemon. It enables making a VPN connection to your devices from within the web browser.

Technical Assistance If you have any questions regarding this Product Advisory, please contact Technical Support at 770-844-4200 or 800-633-0405 for further assistance.