ADV-2026-08-05 - VPN Client Remote Code Execution

Severity	Critical
CVSS 3.1	9.6 — CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H
CVE	CVE-2026-75925
Published	5 August 2026
Advisory version	1.2
Action	Update the IXON VPN Client to v1.4.7 or later or uninstall it. Affected versions can no longer connect, an update is required to restore remote access.

1. Summary

IXON has fixed a critical vulnerability in the IXON VPN Client during internal security testing of its own products. The vulnerability would allow an attacker to perform remote code execution on the computer running the client with elevated privileges.

IXON Cloud no longer accepts VPN clients that are not version 1.4.7 or later, preventing the vulnerability from being exploited.

We have no indication that the vulnerability was exploited, and we are aware of no public disclosure or exploit for it.

2. Affected versions

Affected	IXON VPN Client v1.4.6 and older, on Windows, Linux and macOS
Fixed in	v1.4.7 and later
Not affected	IXON Cloud and IXON Edge Gateways

The client is installed per user. Check your systems for installations, including equipment used by contractors and service partners.

3. What IXON has done

- Released the fixed version, v1.4.7, within 24 hours of confirming the vulnerability
- Prevent the vulnerability from being triggered on computers that have not been updated
- Blocked IXON Cloud from accepting versions below v1.4.7
- Removed all affected versions from distribution, so they can no longer be installed

4. Recommended actions

Update the IXON 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.

5. Additional information

- **CVE ID**: CVE-2026-75925 — https://www.cve.org/CVERecord?id=CVE-2026-75925
- **CISA ICS Advisory**: ICSA-26-246-02 https://www.cisa.gov/news-events/ics-advisories/icsa-26-246-02
- **Credits**: identified internally by Luuk van Rheden, IXON
- **Trust Center**: https://trust.ixon.cloud
- **IXON Security Advisories**: https://trust.ixon.cloud/item/security-advisories