CHECKLIST · SCAMS & SECURITY

Ivanti VPN attacks: a fully patched Connect Secure was broken into, and one flaw is still open

Published 15 October 2026. Read the full story, sources and any updates at
digitaladvisors.com.au/journal/ivanti-connect-secure-zero-day-october-2026/

- [ ] **Find out whether you use Ivanti Connect Secure.** Ask your IT provider which product staff use for remote VPN access.
- [ ] **Get the running version in writing.** Have the provider confirm it is 22.8R2.5, 25.1.1.2, 25.1.3.0 or 25.1.3.1, or a later version Ivanti's advisory lists as fixed.
- [ ] **Ask for a compromise check, not just a patch.** Ask what was checked beyond Ivanti's Integrity Checker Tool, which missed the attack Volexity investigated.
- [ ] **Plan for the second fix.** Ask who will install Ivanti's privilege escalation patch when it is released, and how quickly.
- [ ] **Reset credentials if compromise is found.** Have the provider change passwords and keys reachable from the VPN, including the local administrator passwords and BitLocker recovery keys the attacker searched for.
- [ ] **Report anything suspicious.** Use ReportCyber at cyber.gov.au if your provider finds signs of compromise.

NOTES

General information only, not legal, tax or financial advice. Check the full story and its sources before acting.