

CISA Advises Immediate Action on Ivanti Connect Secure Vulnerability



CISA has identified a critical vulnerability in Ivanti Connect Secure that is being actively exploited. Organizations are urged to patch their systems immediately to prevent unauthorized access and data theft.

- CVE-2026-104935 affects Ivanti Connect Secure versions 25.1.1.1 and earlier.
- The vulnerability allows remote, unauthenticated command execution.
- CISA recommends immediate upgrades to the latest version.
- Organizations should conduct forensics to check for signs of compromise.
- End of life for version 22.8 is January 31, 2027.

Overview

CISA has issued an alert regarding a newly discovered vulnerability in Ivanti Connect Secure, designated as CVE-2026-104935. This vulnerability is being exploited by cyber threat actors to bypass authentication, enabling them to execute arbitrary commands remotely without authentication.

Recommended Actions

Organizations using affected versions of Ivanti Connect Secure are strongly advised to take immediate action. CISA emphasizes the importance of updating to the latest version as per Ivanti's security advisory. Additionally, organizations should review the compatibility guide for detailed patching instructions.

For those concerned about potential compromise, conducting thorough network and memory forensics is essential to identify any exploitation evidence. Note that Ivanti's Integrity Checker Tool may not detect this specific vulnerability.

Steps to Mitigate Risk

If a compromise is suspected, organizations should follow these recovery procedures:

- Create a backup of the appliance configuration.
- Conduct a factory reset and upgrade to the latest version.
- For cloud and virtual systems, rebuild the virtual instance and upgrade.
- Restore the appliance configuration from the backup.
- Reset passwords for all accounts and revoke stored certificates.
- Reset API keys and license server credentials.

By taking these steps, organizations can significantly reduce their risk of exploitation and enhance their overall security posture.

What to do now

1. Update Ivanti Connect Secure to the latest version immediately.
2. Review the Ivanti security advisory for detailed patching guidance.
3. Conduct network and memory forensics to check for exploitation signs.
4. Create backups of appliance configurations.
5. Reset passwords and revoke stored credentials.