

CISA urges immediate Ivanti Connect Secure patching after 105 honeypot exploit attempts



CISA has called for immediate updates to Ivanti Connect Secure appliances following active exploitation of an authentication bypass vulnerability tracked as CVE-2026-104935.

- CISA issued an urgent advisory for Ivanti Connect Secure appliances following disclosure of CVE-2026-104935, an authentication bypass vulnerability with a CVSS score of 8.6
- Honeypot systems recorded 105 exploit attempts, confirming active exploitation in the wild
- Organizations are urged to update ICS deployments to the latest version immediately
- The vulnerability allows attackers to bypass authentication controls on affected appliances

Active exploitation confirmed

The U.S. Cybersecurity and Infrastructure Security Agency has issued an urgent advisory calling on organizations to immediately update Ivanti Connect Secure appliances. The warning follows the disclosure of **CVE-2026-104935**, an authentication bypass vulnerability carrying a CVSS severity score of 8.6. CISA's alert comes after honeypot monitoring systems recorded 105 distinct exploit attempts, providing concrete evidence that threat actors are actively targeting the flaw in production environments.

Vulnerability details

The security flaw represents an **authentication bypass** weakness affecting Ivanti Connect Secure deployments. This class of vulnerability allows attackers to circumvent normal authentication controls, potentially gaining unauthorized access to protected systems and networks. The relatively high CVSS score reflects the serious risk posed to organizations running vulnerable versions of the appliance.

Immediate action required

CISA has emphasized the urgency of applying available updates to all ICS appliances and deployments. The combination of active exploitation evidence and the vulnerability's authentication bypass nature makes this a time-sensitive security matter. Organizations using Ivanti Connect Secure for remote access or VPN services should prioritize patching activities, particularly given the appliance's typical role as a network perimeter control point. Regulated institutions in Saudi Arabia should treat this as a critical infrastructure protection issue requiring immediate attention from security operations teams.

What to do now

1. Immediately inventory all Ivanti Connect Secure appliances deployed in your environment
2. Apply the latest vendor-supplied security updates to all ICS instances without delay
3. Review authentication and access logs for any suspicious activity or unauthorized access attempts during the exposure window
4. Implement enhanced monitoring on all remote access and VPN infrastructure until patching is complete
5. Notify the National Cybersecurity Authority if any indicators of compromise are detected
6. Document patching activities and timelines for compliance and audit purposes