Exploitation of New Ivanti VPN Zero-Day Linked to Chinese Cyberspies

Overview

A newly discovered zero-day vulnerability, CVE-2025-0282 (CVSS 9), has been actively exploited in the wild, primarily targeting Ivanti Connect Secure (ICS) VPN appliances. The flaw allows for unauthenticated attackers to remotely execute arbitrary code on vulnerable devices. Ivanti released patches for this vulnerability alongside another related flaw, CVE-2025-0283 (CVSS 7).

The exploitation of CVE-2025-0282 has been linked to Chinese cyber-espionage activity. The security company Mandiant published findings revealing that these attacks began in mid-December 2024, leveraging the vulnerability to deploy malware and establish persistent access.

- **CVE-2025-0282**
  - Type - Stack-based buffer overflow
  - Impact - Allows unauthenticated remote attackers to execute arbitrary code.
  - Affected Products:
    - Ivanti Connect Secure prior to version 22.7R2.5
    - Ivanti Policy Secure prior to version 22.7R1.2
    - Ivanti Neurons for ZTA gateways prior to version 22.7R2.3
  - Status - Exploited in the wild, primarily on Ivanti Connect Secure appliances.
- **CVE-2025-0283**
  - Type - Privilege escalation
  - Impact: - Allows authenticated local attackers to escalate privileges.
  - Affected Products: Same as CVE-2025-0282.
  - Status - No known exploitation at this time.

While Mandiant has not definitively attributed the activity to a specific threat actor, evidence points to connections with the UNC5337 and UNC5221 espionage groups, which have previously exploited Ivanti products. Aspire recommends patching immediately.

Aspire Protects

- **Patch –** Update Ivanti Connect Secure appliances to version 22.7R2.5 immediately. See Ivanti's advisory for patch guidance.
- For Ivanti Policy Secure and Neurons for ZTA Gateways, implement temporary mitigations and plan for patch deployment on January 21, 2025.
- Conduct internal and external scans using Ivanti's Integrity Checker Tool (ICT).

- If malicious activity is detected, perform a factory reset, update to the latest firmware, and reconfigure appliances securely.
- Monitor for indicators of compromise (IoCs) related to malware families like Spawn, PhaseJam, and DryHook.
- Restrict internet exposure for Ivanti appliances, aligning configurations with vendor recommendations.

TTPs to Watch

Initial Access
- Exploit Public-Facing Application [T1190] – The attacker targeted vulnerable ICS appliances to gain unauthorized access.

Persistence
- Implant Internal Image [T1525] – Malware such as SpawnAnt was used to persist across firmware updates.

Credential Access
- Input Capture [T1056] – The attacker used DryHook to harvest credentials from compromised systems.

Command and Control
- Web Shells [T1505.003] – Web shells were deployed to maintain control over compromised appliances.

IoCs

There are no known IoCs associated with CVE-2025-0282 and CVE-2025-0283 at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

For the Ivanti vulnerabilities (CVE-2025-0282 and CVE-2025-0283), the following industries are likely targeted, based on the history of similar attacks and the deployment of Ivanti Connect Secure (ICS) appliances:

- Government

- Defense Contractors
- Technology
- Media Organizations
- Finance

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

Ivanti Community

Security Update: Ivanti Connect Secure, Policy Secure and Neurons for ZTA Gateways | Ivanti

Ivanti Connect Secure VPN Targeted in New Zero-Day Exploitation | Google Cloud Blog