RESURGE Implant Linked to Active Exploitation of Ivanti Connect Secure

TL;DR

CVE-2025-0282 (CVSS 9) is a remote code execution flaw in Ivanti Connect Secure that has been actively exploited since December 2024.

Attackers used the flaw to drop a malware implant called RESURGE. It can sit quietly on the device, avoid normal monitoring, wipe its own tracks from logs, and even survive reboots. A patch is available, but updating is not enough. Organizations should validate their appliances using Ivanti's Integrity Checker Tool (ICT), as compromised systems may still be infected.

Overview

There is a critical remote code execution vulnerability (CVE-2025-0282, CVSS 9) affecting Ivanti Connect Secure, Ivanti Policy Secure, and Ivanti Neurons for ZTA gateways. The issue is a stack-based buffer overflow that allows an unauthenticated remote attacker to execute code on a vulnerable appliance.

Affected Products

- Ivanti Connect Secure
- Ivanti Policy Secure
- Ivanti Neurons for ZTA Gateways

Affected Versions

- Connect Secure prior to 22.7R2.5
- Policy Secure prior to 22.7R1.3
- Neurons for ZTA prior to 22.8R2

Note - Cloud ZTA gateways were automatically updated as of January 18, 2025.

Exploitation began as a zero-day in mid-December 2024 and has been linked to a China-aligned threat cluster tracked as UNC5221. Following exploitation, attackers deployed a Linux shared object implant named `libdsupgrade.so`, referred to by the Cybersecurity and Infrastructure Security Agency (CISA) as RESURGE.

RESURGE does not operate like typical malware. Rather than reaching out to a command server, it stays quiet and waits for a specific inbound TLS connection from the operator. The implant hooks into the web process, inspects inbound TLS traffic, and only activates if the connection matches a specific fingerprint. If not, traffic passes through normally to the legitimate Ivanti service.

The implant also uses a forged Ivanti certificate during authentication to verify communication with the operator. The certificate is transmitted unencrypted, which provides defenders with a possible network detection opportunity.

Additional capabilities observed:

- Log tampering through `liblogblock.so`
- Credential harvesting and account manipulation
- Password resets and privilege escalation
- Firmware modification and boot-level persistence via `dsmain`

Because the implant can remain dormant until an operator reconnects, compromised devices may appear normal during routine monitoring. Ivanti also addressed CVE-2025-0283 (CVSS 7), a local authenticated privilege escalation vulnerability. There are no confirmed reports of CVE-2025-0283 being exploited in the wild. Aspire recommends patching CVE-2025-0282 as soon as possible.

Aspire Protects

- **Patch** - Upgrade immediately to the fixed software release. See Iva
- Run the updated Integrity Checker Tool (ICT-V22725 build 3819)
- Perform factory reset if ICT indicates compromise
- Review inbound TLS connections for anomalies
- Monitor for log gaps or unexpected certificate behavior

TTPs to Watch

Initial Access

- Exploit Public-Facing Application [T1190] – The attacker may have exploited CVE-2025-0282 in an internet-facing Ivanti Connect Secure appliance to achieve remote code execution.

Persistence

- Boot or Logon Autostart Execution [T1547] – The attacker may have modified system components and firmware to maintain persistence across reboots.

Defense Evasion

- Indicator Removal on Host [T1070] – The attacker may have deployed log-tampering functionality (e.g., liblogblock.so) to remove or alter logs and conceal activity.

- Rootkit [T1014] – The RESURGE implant may function with rootkit-like capabilities to intercept system calls and hide malicious activity.

Command and Control

- Encrypted Channel [T1573] – The attacker may have established a mutual TLS session using elliptic curve encryption for covert command and control.

Behavioral IoCs

Organizations should review:

Appliance File System

- Presence of libdsupgrade.so
- Presence of liblogblock.so
- Presence of dsmain

Network Traffic

- Inbound TLS sessions with unusual certificate behavior
- Suspicious CRC32 TLS fingerprint patterns
- Unexpected mutual TLS handshakes

Logs

- Missing debug or authentication logs
- Sudden log truncation
- Unexplained administrative account activity

Targeted Industries

This vulnerability threatens any organization using Ivanti appliances to manage remote access into corporate networks.

- Education
- Energy
- Finance
- Healthcare
- Legal

- Manufacturing
- Public Sector
- Retail

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

Security Advisory Ivanti Connect Secure, Policy Secure & ZTA Gateways (CVE-2025-0282, CVE-2025-0283)