Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Critical Ivanti Zero-day Flaw Exploited in the Wild

Date of Publication	Last Updated Date	Admiralty Code	TA Number
January 10, 2025	January 21, 2025	A1	TA2025008

Summary

First Seen: December 2024
Affected Product: Ivanti Connect Secure, Policy Secure, and ZTA Gateways
Threat Actor: UNC5337
Threat Cluster: CL-UNK-0979
Malware: DRYHOOK, PHASEJAM, SPAWNANT, SPAWNMOLE, SPAWNSNAIL, SPAWNSLOTH
Impact: Two critical vulnerabilities, CVE-2025-0282 and CVE-2025-0283, have been identified in Ivanti's Connect Secure VPN appliances, with active exploitation detected since December 2024. CVE-2025-0282 enables unauthenticated remote code execution via a buffer overflow, while CVE-2025-0283 allows privilege escalation. These vulnerabilities pose significant risks to organizations relying on these systems for secure remote access.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-0282	Ivanti Connect Secure, Policy Secure, and ZTA Gateways Stack-Based Buffer Overflow Vulnerability	Ivanti Connect Secure, Policy Secure, and ZTA Gateways	✓	✓	✓
CVE-2025-0283	Ivanti Connect Secure, Policy Secure, and ZTA Gateways Stack-Based Buffer Overflow Vulnerability	Ivanti Connect Secure, Policy Secure, and ZTA Gateways	✗	✗	✓

Vulnerability Details

#1

Ivanti has recently reported active exploitation of two critical vulnerabilities, CVE-2025-0282 and CVE-2025-0283, which affect its Connect Secure (ICS) VPN appliances. These vulnerabilities have been exploited in the wild since December 2024, posing significant risks to organizations that rely on these systems for secure remote access.

#2

CVE-2025-0282 is characterized as an unauthenticated stack-based buffer overflow vulnerability. It allows attackers to execute arbitrary code remotely without requiring any authentication. The exploitation method involves sending specially crafted inputs to the appliance, resulting in a memory overflow that enables the attacker to gain control over the system. This can facilitate various malicious activities, including malware deployment and network compromise.

#3

CVE-2025-0283 is another stack-based buffer overflow vulnerability affecting the same Ivanti products and versions as CVE-2025-0282. However, exploitation of this vulnerability requires local authenticated access, enabling an attacker to escalate their privileges on the system. It may be exploited in conjunction with CVE-2025-0282, allowing attackers to execute more complex attacks.

#4

Researchers have observed that attackers are leveraging CVE-2025-0282 for remote code execution by first conducting reconnaissance to identify vulnerable appliance versions. Once identified, they send crafted payloads that trigger the buffer overflow, modify system settings to facilitate malware installation, and inject web shells into legitimate components for persistent access.

#5

Notably, these attacks have been linked to various malware families, including DRYHOOK, PHASEJAM and SPAWN ecosystem (which includes the SPAWNANT installer, SPAWNMOLE tunneler and the SPAWNSNAIL SSH backdoor and SPAWNSLOTH log tampering utility), indicating a coordinated effort by multiple threat actors, notably the China-nexus group UNC5337.

#6

CL-UNK-0979 is a threat cluster exploiting Ivanti's CVE-2025-0282 vulnerability, enabling access, credential harvesting, lateral movement via RDP, and persistence with tools like SPAWNSNAIL. Attackers evade detection by deleting logs and clearing directories. While overlaps exist with UNC5337 activity, there isn’t enough evidence to confirm the same actor.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-0282	Ivanti Connect Secure: 22.7R2 through 22.7R2.4 Ivanti Policy Secure: 22.7R1 through 22.7R1.2 Ivanti Neurons for ZTA gateways: 22.7R2 through 22.7R2.3	cpe:2.3:a:ivanti:connect_secure:*:*:*:*:*:*:* cpe:2.3:a:ivanti:policy_secure:*:*:*:*:*:*:* cpe:2.3:a:ivanti:neurons_for_zta_gateways:*:*:*:*:*:*:*	CWE-121
CVE-2025-0283	Ivanti Connect Secure: 22.7R2.4 and prior, 9.1R18.9 and prior Ivanti Policy Secure: 22.7R1.2 and prior Ivanti Neurons for ZTA gateways: 22.7R2.3 and prior	cpe:2.3:a:ivanti:connect_secure:*:*:*:*:*:*:* cpe:2.3:a:ivanti:policy_secure:*:*:*:*:*:*:* cpe:2.3:a:ivanti:neurons_for_zta_gateways:*:*:*:*:*:*:*	CWE-121

Recommendations

Apply Security Patches Immediately: Upgrade Ivanti Connect Secure to version 22.7R2.5 or later, Ivanti Policy Secure to version 22.7R1.3 or later, and Neurons for ZTA Gateways to version 22.8R2 or later. For Neurons for ZTA Gateways deployed as a cloud service, updates were automatically applied as of January 18, 2025.Monitor Ivanti's security advisories for patch updates and apply them promptly.

Conduct Integrity Checks: Use Ivanti's Integrity Checker Tool (ICT) to detect unauthorized modifications or exploitation. Run the ICT regularly, especially after patching, to verify the integrity of the system.

Review and Harden Access Controls: Limit administrative access to Ivanti devices using strict role-based access control (RBAC). Enforce multi-factor authentication (MFA) for all remote and administrative access. Disable unnecessary services and ports to reduce the attack surface.

Network Segmentation: Isolate Ivanti appliances from sensitive parts of your network. Restrict access to Ivanti devices using firewalls and VPNs, allowing only trusted IP ranges.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0042 Resource Development	TA0002 Execution	TA0004 Privilege Escalation
TA0006 Credential Access	TA0008 Lateral Movement	TA0005 Defense Evasion	TA0003 Persistence
TA0011 Command and Control	T1071.001 Web Protocols	T1071 Application Layer Protocol	T1574 Hijack Execution Flow
T1059 Command and Scripting Interpreter	T1588.006 Vulnerabilities	T1588 Obtain Capabilities	T1588.005 Exploits

T1190 Exploit Public-Facing Application	**T1565** Data Manipulation	**T1068** Exploitation for Privilege Escalation	**T1505.003** Web Shell
T1003 OS Credential Dumping	**T1070** Indicator Removal	**T1562.001** Disable or Modify Tools	**T1562** Impair Defenses
T1555 Credentials from Password Stores	**T1552** Unsecured Credentials	**T1021.001** Remote Desktop Protocol	**T1021** Remote Services
T1070.004 File Deletion	**T1070** Indicator Removal	**T1543.003** Windows Service	**T1574.002** DLL Side-Loading

Indicators of Compromise (IOCs)

TYPE	VALUE
File Paths	/tmp/s, /home/webserver/htdocs/dana-na/jam/getComponent.cgi, /home/webserver/htdocs/dana-na/auth/restAuth.cgi, /root/home/lib/libsshd.so, /root/home/lib/libsocks5.so, /root/lib/libupgrade.so, /tmp/.liblogblock.so
MD5	E7d24813535f74187db31d4114f607a1, A638fd203ddb540d0484d8e00490df06, D18e5425ecd9608ecb992606b974e15d, 61bb586dc4e047ab081ef6ca65684e48
SHA256	4d7f4c330cdb4c16de4327b1b82f3cbe53d20c117fffc972a2d3a47e01e0a65f, 7144B8C77D261985205AE2621EB6242F43D6244E18B8D01D05048337346B6EFD, AAE291AC5767CFE93676DACB67BA50C98D8FD520F5821FB050FD63E38B000B18, 366635c00b8e6f749a4d948574a0f1e7b4c842ca443176de27af45debbc14f71, 3526af9189533470bc0e90d54bafb0db7bda784be82a372ce112e361f7c7b104, 43363AA0D1FDAB0174D94BD5A9E16D47CBB08B4B089C5A12E370133AB8E640A6,

TYPE	VALUE
SHA256	1dc0a3a5904ec35103538a018ef069fbe95b0a3c26cb0ff9ba0d1c268d1aaf98, f9ca95119b32a18491e3cc28c7020ee00f6e7a45ae089c876d87252e754e5a2e, 723711ccbb3eaf1daea3d5b00aa6aaee48a359be395d9500d8a56609ec5238e9, 75a3d53c1d63ecb338d4b2d6f5b3d980b0caceb77808ed81ab73b49138cc0a26, a6b24fcef2e018c9ef634aa21e26a74ff94ea508a8b132fad38d48f5ab10fcd3
IPv4	185[.]219[.]141[.]95, 185[.]195[.]71[.]244, 193[.]149[.]180[.]128, 168[.]100[.]8[.]144
Host name	DESKTOP-1JIMIV3

Patch Details

- Ivanti Connect Secure: Upgrade to version 22.7R2.5 immediately.
- Ivanti Policy Secure: Upgrade to version 22.7R1.3 or later.
- Neurons for ZTA Gateways: Upgrade to version 22.8R2 or later. For cloud deployments, note that services were automatically updated as of January 18, 2025.

Link:
https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283

References

https://www.ivanti.com/blog/security-update-ivanti-connect-secure-policy-secure-and-neurons-for-zta-gateways

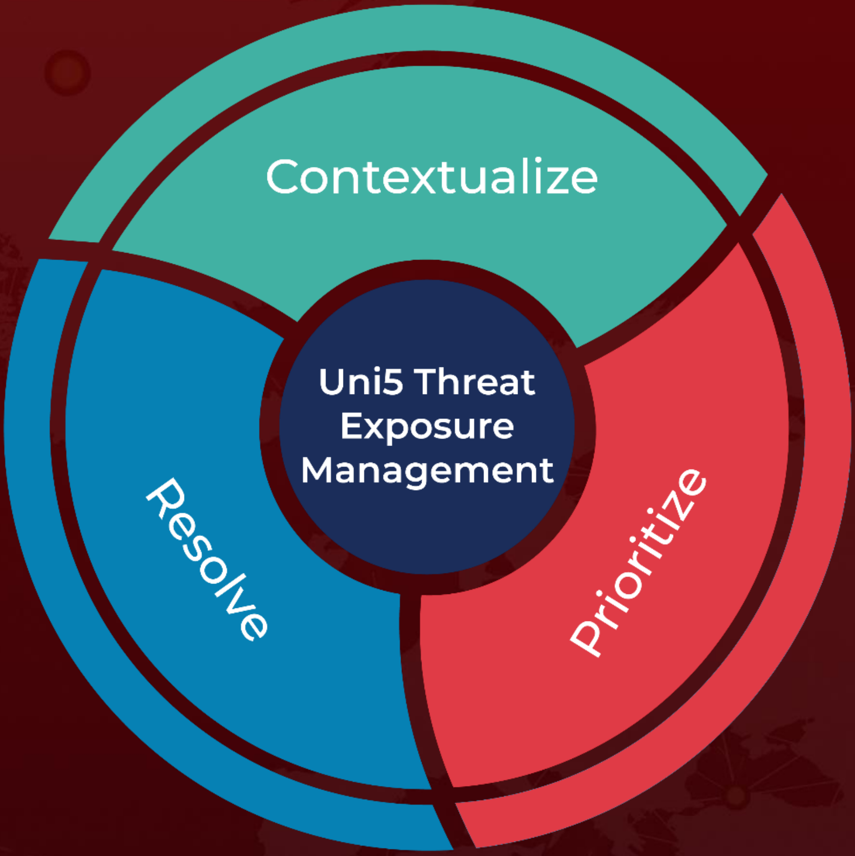
https://cloud.google.com/blog/topics/threat-intelligence/ivanti-connect-secure-vpn-zero-day

https://unit42.paloaltonetworks.com/threat-brief-ivanti-cve-2025-0282-cve-2025-0283/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

January 10, 2025 • 3:30 AM

More at www.hivepro.com