

HiveForce Labs

THREAT ADVISORY



VULNERABILITY REPORT

CVE-2025-22457: Hackers Actively Exploiting Ivanti's Critical New Flaw

Date of Publication

April 4, 2025

Admiralty Code

A1

TA Number

TA2025102

Summary

First Seen: April 3, 2025

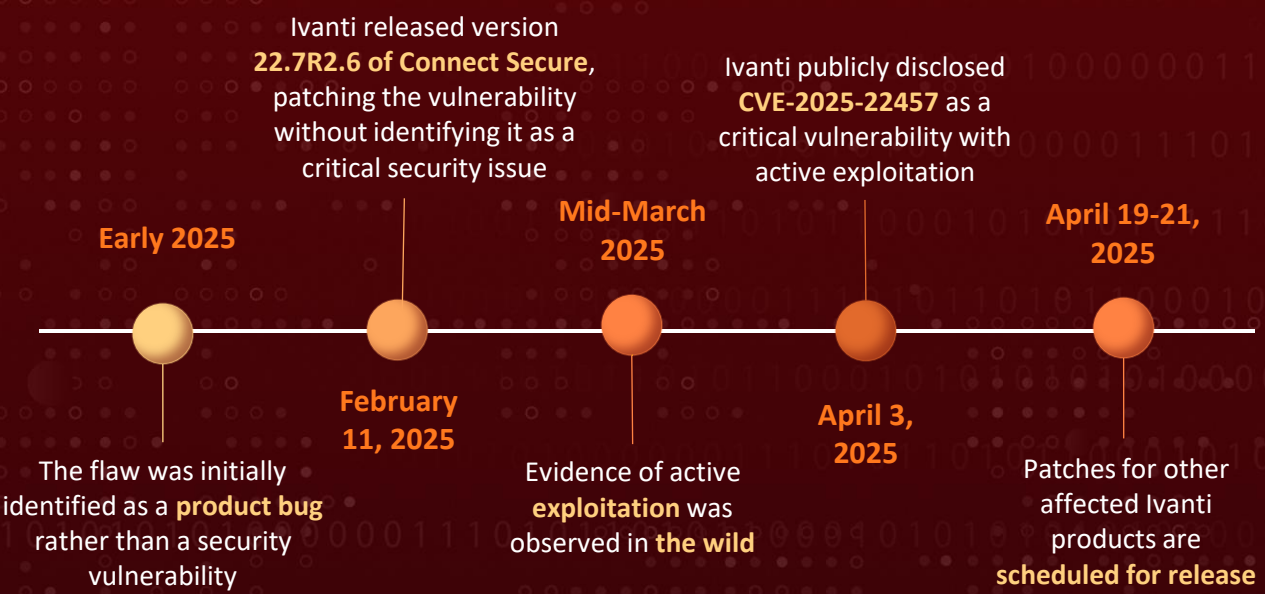
Affected Product: Ivanti Connect Secure, Policy Secure, and ZTA Gateways

Malware: TRAILBLAZE, BRUSHFIRE, SPAWNSNARE, SPAWNWAVE, SPAWNSLOTH




Threat Actor: UNC5221

Impact: Ivanti disclosed a critical vulnerability (CVE-2025-22457) affecting Ivanti Connect Secure, Pulse Connect Secure, and other gateway products. The stack-based buffer overflow flaw enables remote, unauthenticated attackers to execute arbitrary code. Initially seen as a low-risk bug and patched in February 2025, it has been actively exploited since mid-March by suspected Chinese threat actors deploying TRAILBLAZE and BRUSHFIRE malware. Ivanti patched Connect Secure in v22.7R2.6, and organizations must update or migrate unsupported systems immediately.

Vulnerability Timeline



CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-22457	Ivanti Connect Secure, Policy Secure, and ZTA Gateways Stack-Based Buffer Overflow Vulnerability	Ivanti Connect Secure, Policy Secure, and ZTA Gateways			

Vulnerability Details

#1

A significant stack-based buffer overflow vulnerability, CVE-2025-22457, was discovered in several Ivanti products, including Ivanti ZTA Gateways, Ivanti Connect Secure, and Ivanti Policy Secure. Due to its small character set, it was initially mistaken for a denial-of-service issue. However, further research revealed that the vulnerability could be exploited to remotely execute malware without authentication.

#2

Security researchers recently uncovered active exploitation of this vulnerability. Evidence suggests that as early as mid-March 2025, a suspected China-nexus threat actor, tracked as [UNC5221](#), exploited the flaw to deploy custom malware. This actor, known for leveraging both zero-day and n-day vulnerabilities against network edge devices, in this incident they utilized a multi-stage shell script dropper to trigger the in-memory-only TRAILBLAZE dropper, which then injected the BRUSHFIRE passive backdoor into running processes. Further analysis linked this sophisticated attack chain to additional malware components from the SPAWN ecosystem.

#3

The vulnerability affects Ivanti Connect Secure versions 22.7R2.5 and earlier, with a full patch released in version 22.7R2.6 on February 11, 2025. Ivanti Policy Secure and Ivanti ZTA Gateways are also impacted, with patches scheduled for future releases. Additionally, end-of-support Pulse Connect Secure 9.x appliances remain vulnerable, as they stopped receiving updates after December 31, 2024.

#4

In response, Ivanti has released patches for Ivanti Connect Secure, with version 22.7R2.6 fully addressing the issue. Patches for Ivanti Policy Secure and Ivanti ZTA Gateways are expected soon. Organizations using Pulse Connect Secure, which is no longer supported, are strongly advised to migrate to a supported solution immediately.



Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-22457	Ivanti Connect Secure: 22.7R2.5 and prior Pulse Connect Secure (EoS): 9.1R18.9 and prior Ivanti Policy Secure: 22.7R1.3 and prior ZTA Gateways: 22.8R2 and prior	cpe:2.3:a:ivanti:connect_secure:*:*:*:*:* cpe:2.3:a:ivanti:neurons_for_zta_gateways:*:*:*:*:* cpe:2.3:a:ivanti:policy_secure:*:*:*:*:*	CWE-121



Recommendations



Immediate Patching: Upgrade Ivanti Connect Secure to version 22.7R2.6 or later as soon as possible. This version includes the patch for CVE-2025-22457.



Migration for End-of-Support Products: For Pulse Connect Secure 9.1x, which is now End-of-Support, migrate to a supported Ivanti platform to ensure security updates are available.



Monitor for Compromise: Use the Integrity Checker Tool (ICT) to monitor for signs of exploitation. If suspicious activity is detected, perform a factory reset on the appliance before reinstalling with a patched version.



Factory Reset if Compromised: If signs of compromise are detected, perform a factory reset on affected appliances and reinstall using patched versions to eliminate any persistent malware or unauthorized modifications.



Vulnerability Management Program: Establish a robust vulnerability management program that includes continuous scanning, risk-based prioritization, remediation, validation, and reporting. This lifecycle approach ensures vulnerabilities are systematically addressed and mitigated.



Potential MITRE ATT&CK TTPs

<u>TA0042</u> Resource Development	<u>TA0001</u> Initial Access	<u>TA0002</u> Execution	<u>TA0004</u> Privilege Escalation
<u>TA0005</u> Defense Evasion	<u>TA0003</u> Persistence	<u>TA0011</u> Command and Control	<u>T1068</u> Exploitation for Privilege Escalation
<u>T1588</u> Obtain Capabilities	<u>T1190</u> Exploit Public-Facing Application	<u>T1588.005</u> Exploits	<u>T1588.006</u> Vulnerabilities
<u>T1070.004</u> File Deletion	<u>T1070</u> Indicator Removal	<u>T1027</u> Obfuscated Files or Information	<u>T1204</u> User Execution
<u>T1059</u> Command and Scripting Interpreter			



✂ Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	4628a501088c31f53b5c9ddf6788e835, E5192258c27e712c7acf80303e68980b, 6e01ef1367ea81994578526b3bd331d6, Ce2b6a554ae46b5eb7d79ca5e7f440da, 10659b392e7f5b30b375b94cae4fdca0
File Path	/tmp/.i, /tmp/.r, /bin/dsmain, /lib/libdsupgrade.so, /tmp/.liblogblock.so

✂ Patch Details

- Ivanti Connect Secure: Patched in version 22.7R2.6 (released Feb 11, 2025), fully mitigates the issue.
- Ivanti Policy Secure: Patch 22.7R1.4 scheduled for April 21, 2025 to fix the vulnerability.
- Ivanti ZTA Gateways: Patch 22.8R2.2 scheduled for April 19, 2025 to address the flaw.
- Pulse Connect Secure: No patch available (End-of-support Dec 31, 2024), requires migration.

Link:

<https://forums.ivanti.com/s/article/April-Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-22457>

✂ References

<https://forums.ivanti.com/s/article/April-Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-22457>

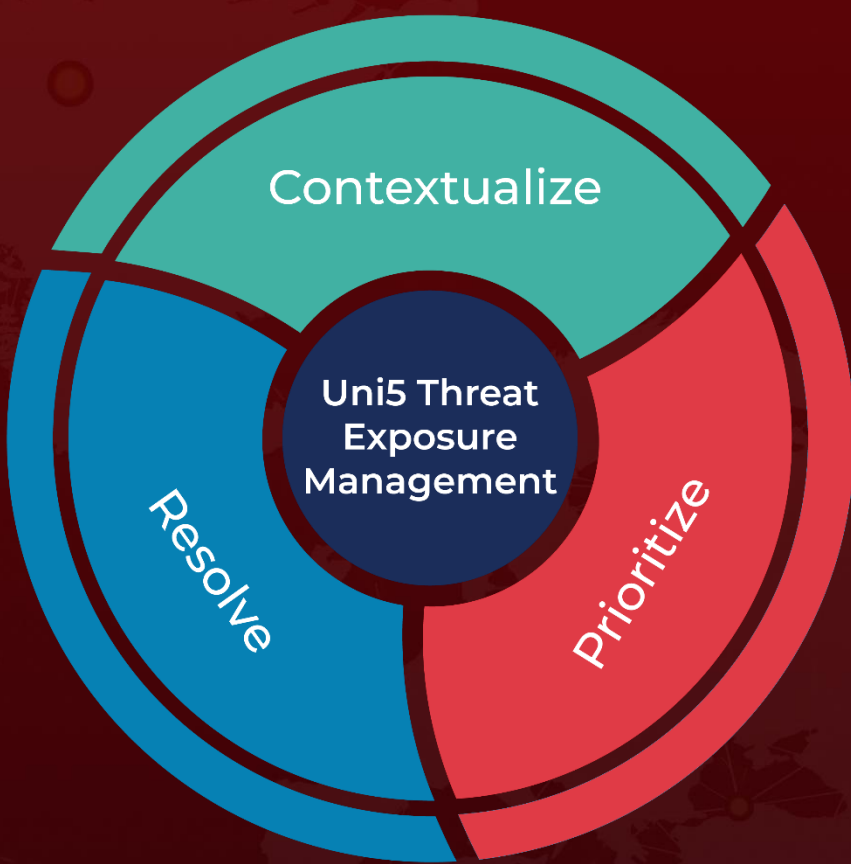
<https://cloud.google.com/blog/topics/threat-intelligence/china-nexus-exploiting-critical-ivanti-vulnerability>

<https://www.hivepro.com/threat-advisory/two-zero-day-flaws-found-in-ivanti-connect-secure-and-policy-secure/>

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
April 4, 2025 • 6:30 AM

