THREAT BULLETINS

Ivanti Connect Secure Vulnerability Actively Exploited by China-Nexus Group

TLP:WHITE

Apr 03, 2025

On April 3, 2025, Ivanti released a security advisory regarding the active exploitation of a critical security flaw affecting vulnerable Ivanti Connect Secure, Pulse Connect Secure, Policy Secure, and ZTA gateway products.

The vulnerability, tracked as CVE-2025-22457, has a CVSS critical score of 9.0 and is a stack-based buffer overflow flaw impacting Ivanti Connect Secure (22.7R2.5 and prior), Pulse Connect Secure (9.1R18.9 and prior) which reached end-of-support as of December 31, 2024, Ivanti Policy Secure (22.7R1.3 and prior), and ZTA Gateways (22.8R2 and prior).

Successful exploitation of the security flaw allows remote unauthenticated threat actors to gain remote code execution capabilities on vulnerable instances.

According to Mandiant and Ivanti, evidence of active exploitation in the wild has been observed against Ivanti Connect Secure 9.x (end of life) and 22.7R2.5 and earlier versions.

Health-ISAC provides this information to increase situational awareness and encourages users to upgrade affected Ivanti products to remediate the vulnerability.

The first sighting of active exploitation occurred in mid-March 2025, following a successful compromise. Two newly identified malware families were observed, TRAILBLAZE and BRUSHFIRE, which are identified as an in-memory dropper and a passive backdoor, respectively.

Following successful exploitation, Mandiant researchers observed a shell script that executed the TRAILBLAZE dropper. This led to the BRUSHFIRE passive backdoor being launched in a critical process of Ivanti Connect Secure to execute follow-on activity. Additionally, the SPAWN ecosystem of malware was deployed, along with a modified version of the Integrity Checker Tool (ICT) for detection evasion.

Given the subsequent deployment of the SPAWN ecosystem of malware after successfully exploiting CVE-2025-22457, Google Threat Intelligence Group (GTIG) has attributed the observed activity to UNC5221. This group has a history of targeting edge devices and has been observed conducting zero-day exploitation.

Recommendations:

Health-ISAC recommends organizations review and assess their level of risk to this vulnerability and take the necessary actions to ensure risk mitigations are implemented, including:

- Immediately applying the available patch to remediate CVE-2025-22457
- Using the external and internal Integrity Checker Tool (ICT)
- Actively monitoring for suspicious activity
- Reviewing the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients Resources.

Reference(s)	Google Threat Horizons Report, Google Threat Horizons Report, Security Week, Security Online, Australian Government
Vendors	Ivanti

Alert ID 3e007f64

View Alert

Share Feedback

was this helpful? |

Tags Google Threat Intelligence Group, ZTA Gateway, CVE-2025-22457, Ivanti Connect Secure, Policy Secure, Mandiant, Ivanti, Pulse Connect Secure

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Access the Health-ISAC Threat Intelligence Portal
Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments
Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**