BREAKING CYBERSECURITY NEWS: CHINA-BACKED ESPIONAGE GROUP HITS IVANTI CUSTOMERS AGAIN

Vairav Cyber Security News Report

Date: April 4, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Thirbam Sadak 148
Baluwatar, Kathmandu

EXECUTIVE SUMMARY

A Chinese state-sponsored espionage group, tracked as UNC5221, has been actively exploiting a critical vulnerability (CVE-2025-22457) in Ivanti's Connect Secure VPN products since mid-March 2025. This exploitation allows for unauthenticated remote code execution, potentially leading to unauthorized access and control over affected systems. Organizations utilizing vulnerable versions of Ivanti's VPN products are at significant risk of data breaches and operational disruptions.

DETAILS OF THE INCIDENT

Description of the Cyber Threat: The attack exploits a stack-based buffer overflow vulnerability (CVE-2025-22457) in Ivanti Connect Secure appliances and Pulse Connect Secure appliances enabling attackers to execute arbitrary code remotely without authentication.

Identification: The exploitation was identified by Mandiant in mid-March 2025 during their ongoing threat monitoring activities. Ivanti released a patch for the vulnerability on February 11, 2025, but did not publicly disclose the issue until April 3, 2025.

Threat Actor: UNC5221 is a Chinese state-sponsored Advanced Persistent Threat (APT) group known for targeting network edge devices and exploiting vulnerabilities in Ivanti products.

Affected Entities/Industries: Organizations utilizing the following Ivanti VPN products have been exploited:

- Ivanti Connect Secure 22.7R2.5 or earlier versions.
- Pulse Connect Secure 9.1x appliances.

Potential Impact:

- **Unauthorized Access**: Exploitation can lead to unauthorized access to sensitive data and systems.

- **Operational Disruption**: Attackers may disrupt business operations by manipulating or disabling critical systems.
- **Data Breaches**: Potential exposure of confidential information, leading to reputational damage and legal consequences.

Exploitation Methods: The attackers exploit the stack-based buffer overflow vulnerability to achieve remote code execution, allowing them to install malware, exfiltrate data, and maintain persistent access to compromised systems.

RECOMMENDED ACTIONS

Immediate Mitigation Steps

- Update Ivanti Connect Secure appliances to version 22.7R2.6 or later to remediate the vulnerability.
- Update Ivanti Policy Secure appliances to version 22.7R1.4.
- Update Ivanti ZTA Gateways to 22.8R2.2.
- For Pulse Connect Secure 9.1x appliances, which are no longer supported, consider upgrading to supported versions or replacing them with supported hardware.

Security Best Practices

- Regularly apply security patches and updates to all software and hardware components.
- Monitor network traffic for unusual activity indicative of exploitation attempts.
- Implement robust access controls and multi-factor authentication to limit unauthorized access.

For Advanced Security Teams

- Conduct thorough threat hunting activities focusing on Ivanti appliance logs and network traffic.
- Utilize endpoint detection and response (EDR) tools to identify and mitigate potential compromises.

- Collaborate with threat intelligence providers to stay updated on emerging threats and IOCs related to UNC5221.

ADDITIONAL RESOURCES AND OFFICIAL STATEMENTS

- https://cyberscoop.com/china-espionage-group-ivanti-vulnerability-exploits/
- https://app.opencve.io/cve/CVE-2025-22457
- https://forums.ivanti.com/s/article/April-Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-22457?language=en_US

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com