NATIONAL CSIRT-CY

**CVE-2025-22457** **04/04/2025**

**Critical Ivanti Vulnerability (CVE-2025-22457)**

## Executive Summary

CVE-2025-22457 is a critical stack-based buffer overflow vulnerability affecting multiple Ivanti products, including Connect Secure (ICS), Policy Secure (IPS), and ZTA Gateways. The flaw allows remote unauthenticated attackers to execute arbitrary code, potentially leading to full system compromise. It has been actively exploited by the Chinese state-sponsored threat group UNC5221 since mid-March 2025, deploying malware strains such as TRAILBLAZE and BRUSHFIRE for persistent access.

## Analysis

The vulnerability exists due to improper handling of memory operations, leading to a stack-based buffer overflow. Attackers can exploit this flaw to overwrite critical memory areas, leading to arbitrary code execution. Given its unauthenticated remote nature, this vulnerability is particularly dangerous as it allows attackers to compromise devices without user interaction.

UNC5221's exploitation method involves deploying TRAILBLAZE, an in-memory dropper that injects malicious payloads, and BRUSHFIRE, a backdoor that enables stealthy and persistent control over infected systems. The presence of these malware strains indicates a highly sophisticated attack campaign targeting government, financial, and enterprise networks.

## Common Vulnerabilities & Exposures

https://nvd.nist.gov/vuln/detail/CVE-2025-22457

## Versions affected

- **Ivanti Connect Secure (ICS) – Versions prior to 22.7R2.6**
- **Ivanti Policy Secure (IPS) – Versions before 22.7R1.4**
- **Ivanti ZTA Gateways – Versions before 22.8R2.2**

## Solutions

To mitigate CVE-2025-22457, update Ivanti Connect Secure (ICS) to 22.7R2.6+, Policy Secure (IPS) to 22.7R1.4+, and ZTA Gateways to 22.8R2.2+. Monitor for TRAILBLAZE and BRUSHFIRE malware, check logs for unusual activity, and restrict network access. Implement firewalls, IDS, MFA, and conduct security audits. If compromised, isolate affected systems, reset credentials, and follow Ivanti's security advisories for updates.

Please distribute this information among your subsidiaries and partners, and also share with us any pertinent information and findings you may have (e.g IOCs, TTPs etc)

The Digital Security Authority extends its appreciation for the continued collaboration.

## Disclaimer

Organizations are advised to consult with relevant cybersecurity professionals and follow best practices for their specific environments.