Vulnerabilities in Ivanti Connect Secure (ICS), Policy Secure (IPS), and Secure Access Client (ISAC)

Vairav Advisory Report

Date: February 12, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Phone: +977 4541540

Mobile: +977-9820105900

Email: mail@vairavtech.com

Thirbam Sadak 148
Baluwatar, Kathmandu

EXECUTIVE SUMMARY

Ivanti has released updates addressing multiple vulnerabilities in Ivanti Connect Secure (ICS), Ivanti Policy Secure (IPS), and Ivanti Secure Access Client (ISAC). These vulnerabilities range from medium to critical severity, with potential impacts including remote code execution (RCE), arbitrary file access, privilege escalation, and information disclosure. Organizations using affected versions are strongly advised to apply the latest patches immediately.

VULNERABILITY DETAILS

CVE-2024-38657

Description: External control of a file name vulnerability in Ivanti Connect Secure and Policy Secure allows a remote authenticated attacker with admin privileges to write arbitrary files.

Impact: Arbitrary files write

CVSS Score: 9.1 (Critical)

CVE-2025-22467

Description: A stack-based buffer overflow vulnerability in Ivanti Connect Secure allows a remote authenticated attacker to achieve remote code execution.

Impact: Remote Code Execution (RCE).

CVSS Score: 9.9 (Critical)

CVE-2024-10644

Description: Code injection vulnerability in Ivanti Connect Secure and Policy Secure allows a remote authenticated attacker with admin privileges to achieve remote code execution.

Impact: Remote Code Execution (RCE)

CVSS Score: 9.1 (Critical)

CVE-2024-12058

Description: External control of a file name vulnerability in Ivanti Connect Secure and Policy Secure allows a remote authenticated attacker with admin privileges to read arbitrary files.

Impact: Arbitrary file read.

CVSS Score: 6.8 (Medium)

CVE-2024-13830

Description: Reflected cross-site scripting (XSS) vulnerability in Ivanti Connect Secure and Policy Secure allows a remote unauthenticated attacker to obtain admin privileges via user interaction.

Impact: Privilege escalation.

CVSS Score: 6.1 (Medium).

CVE-2024-13842

Description: A hardcoded cryptographic key in Ivanti Connect Secure and Policy Secure allows a local unauthenticated attacker to read sensitive data.

Impact: Information disclosure.

CVSS Score: 6.0 (Medium).

CVE-2024-13843

Description: Cleartext storage of sensitive information vulnerability in Ivanti Connect Secure and Policy Secure allows a local unauthenticated attacker to read sensitive data.

Impact: Information disclosure.

CVSS Score: 6.0 (Medium)

CVE-2024-13813

Description: Insufficient permission controls in Ivanti Secure Access Client allow a local authenticated attacker to delete arbitrary files.

Impact: Privilege escalation, data loss.

CVSS Score: 7.1 (High)

AFFECTED VERSIONS

Ivanti Connect Secure (ICS): 22.7R2.5 and below

Ivanti Policy Secure (IPS): 22.7R1.2 and below

Ivanti Secure Access Client (ISAC): 22.7R4 and below

EXPLOIT DETAILS

Exploiting these vulnerabilities could allow attackers to execute arbitrary code, escalate privileges, read or write sensitive files, or gain unauthorized administrative access. Remote and local attack vectors exist, increasing the risk of compromise.

RECOMMENDED ACTIONS

- Ivanti has released patches to mitigate these vulnerabilities. Users should update to the latest available versions.

REFERENCES

https://forums.ivanti.com/s/article/February-Security-Advisory-Ivanti-Connect-Secure-ICS-Ivanti-Policy-Secure-IPS-and-Ivanti-Secure-Access-Client-ISAC-Multiple-CVEs?language=en_US

https://securityonline.info/cve-2025-22467-cvss-9-9-ivanti-connect-secure-vulnerability-allows-remote-code-execution/

https://nvd.nist.gov/vuln/detail/CVE-2025-22467

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: mail@vairavtech.com

Website: https://vairavtech.com