An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2502120148

NCSC Advisory

Multiple Critical Vulnerabilities in Ivanti Security Products

12th, February 2025

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use **TLP:CLEAR** when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

An Roinn Comhshaoil, Aeráide agus Cumarsáide
Department of the Environment, Climate and Communications

Description

CVE ID and CVSS Score:

- CVE-2025-22467 (CVSS: 9.9)
- CVE-2024-38657 (CVSS: 9.1)
- CVE-2024-10644 (CVSS: 9.1)
- CVE-2024-13813 (CVSS: 7.1)
- CVE-2024-12058 (CVSS: 6.8)
- CVE-2024-13830 (CVSS: 6.1)
- CVE-2024-13842 (CVSS: 6.0)
- CVE-2024-13843 (CVSS: 6.0)

Published: 2025-02-12

Vendor: Ivanti

Products: Ivanti Connect Secure (ICS), Ivanti Policy Secure (IPS) and Ivanti Secure Access Client (ISAC)

Products affected

Product	Version
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

Impact

CVE-2025-22467 (CWE-121): A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.6 allows a remote authenticated attacker to achieve remote code execution.

CVE-2024-38657 (CWE-73): External control of a file name in Ivanti Connect Secure before version 22.7R2.4 and Ivanti Policy Secure before version 22.7R1.3 allows a remote authenticated attacker with admin privileges to write arbitrary files.

CVE-2024-10644 (CWE-94): Code injection in Ivanti Connect Secure before version 22.7R2.4 and Ivanti Policy Secure before version 22.7R1.3 allows a remote authenticated attacker with admin privileges to achieve remote code execution.

CVE-2024-13813 (CWE-732) Insufficient permissions in Ivanti Secure Access Client before version 22.8R1 allows a local authenticated attacker to delete arbitrary files.

CVE-2024-12058 (CWE-73): External control of a file name in Ivanti Connect Secure before version 22.7R2.6 and Ivanti Policy Secure before version 22.7R1.3 allows a remote authenticated attacker with admin privileges to read arbitrary files.

CVE-2024-13830 (CWE-79): Reflected XSS in Ivanti Connect Secure before version 22.7R2.6 and Ivanti Policy Secure before version 22.7R1.3 allows a remote unauthenticated attacker to obtain admin privileges. User interaction is required.

CVE-2024-13842 (CWE-321): A hardcoded key in Ivanti Connect Secure before version 22.7R2.3 and Ivanti Policy Secure before version 22.7R1.3 allows a local unauthenticated attacker to read sensitive data.

CVE-2024-13843 (CWE-312): Cleartext storage of information in Ivanti Connect Secure before version 22.7R2.6 and Ivanti Policy Secure before version 22.7R1.3 allows a local unauthenticated attacker to read sensitive data.

Common Weakness Enumeration (CWE)[1]:

CWE-121: Stack-based Buffer Overflow.

CWE-73: External Control of File Name or Path.

CWE-94: Improper Control of Generation of Code ('Code Injection').

CWE-732: Incorrect Permission Assignment for Critical Resource.

CWE-73: External Control of File Name or Path.

CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting').

[1] https://cwe.mitre.org

CWE-321: Use of Hard-coded Cryptographic Key.

CWE-312: Cleartext Storage of Sensitive Information.

Known Exploited Vulnerability (KEV) catalog[2]: No

Used by Ransomware Operators: N/A

Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from Ivanti.

- https://nvd.nist.gov/vuln/detail/CVE-2025-22467
- https://www.cve.org/CVERecord?id=CVE-2025-22467
- 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

[2] https://www.cisa.gov/known-exploited-vulnerabilities-catalog