An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2502120168

NCSC Advisory

Critical Vulnerability found in Ivanti Cloud Services Application (CSA)

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-2024-47908 (CVSS: 9.1)
- CVE-2024-11771 (CVSS: 5.3)

Published: 2025-02-11

Vendor: Ivanti

Product: Ivanti Cloud Services Application (CSA)

Products affected

Product	Version
Ivanti Cloud Services Application (CSA)	5.0.4 and prior

Impact

CVE-2024-47908 (CWE-78): OS command injection in the admin web console of Ivanti CSA before version 5.0.5 allows a remote authenticated attacker with admin privileges to achieve remote code execution.

CVE-2024-11771 (CWE-22): Path traversal in Ivanti CSA before version 5.0.5 allows a remote unauthenticated attacker to access restricted functionality.

Common Weakness Enumeration (CWE)[1]:

CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection').

CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal').

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

Used by Ransomware Operators: N/A

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

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

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-2024-47908
- https://www.cve.org/CVERecord?id=CVE-2024-47908
- https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Cloud-Services-Application-CSA-CVE-2024-47908-CVE-2024-11771?language=en_US