National Cyber Security Centre

2409200152-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Critical vulnerability in Ivanti CSA (Cloud Services Appliance) (CVE-2024-8963, CVSSv3: 9.4)

Friday 20th September, 2024

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.

Description

CVE ID: CVE-2024-8963
Published: 2024-09-19 17:14:49
Vendor: Ivanti
Product: CSA (Cloud Services Appliance)
CVSS3.x Score[1]**:** 9.4
EPSS[2]**:** 0.979020000
(For up to date EPSS score, see here: https://api.first.org/data/v1/epss?cve=CVE-2024-8963)

Summary: Ivanti is disclosing a critical vulnerability in Ivanti CSA 4.6 which was incidentally addressed in the patch released on 10 September (CSA 4.6 Patch 519). Successful exploitation could allow a remote unauthenticated attacker to access restricted functionality. If CVE-2024-8963 is used in conjunction with CVE-2024-8190 an attacker can bypass admin authentication and execute arbitrary commands.

Products Affected

- Ivanti CSA (Cloud Services Appliance): version 4.6 (all versions prior to patch 519)

Impact

Exploitation of this vulnerability could allow a remote authenticated user to access restricted functionality and execute arbitrary commands.

Common Weakness Enumeration (CWE)[3]**:** CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Present in CISA Known Exploited Vulnerability(KEV)[4] **catalog:** YES
Used by Ransomware Operators: Not Known

Recommendations

The NCSC strongly advises affected organisations to review the latest release notes and install the relevant updates from Ivanti.

Additional recommendations and mitigation's for CVE-2024-8963 can be found in the respective link below:

- https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-CSA-4-6-Cloud-Services-Appliance-CVE-2024-8963;

[1] https://www.first.org/cvss/v3.0/specification-document
[2] https://www.first.org/epss/articles/prob_percentile_bins
[3] https://cwe.mitre.org/
[4] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

DISCLAIMER: This document is provided “as is” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.

National Cyber Security Centre
Tom Johnson House,
Beggars Bush,
Dublin, D04 K7X4,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@ncsc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie

An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre