CYBER ADVISORY

TLP:CLEAR

10 February 2025

Multiple Ivanti Cloud Service Application Vulnerabilities

Ivanti CSA | Exploited in the wild | End-of-Life | Chained Vulnerabilities

The California Cybersecurity Integration Center (Cal-CSIC) has identified ongoing exploitation of multiple vulnerabilities in Ivanti's Cloud Service Applications (CSA) version 4.6, an end-of-life product, with the most critical of the vulnerabilities rated as a 9.4 in CVSS 3.1. These vulnerabilities include CVE-2024-8963, CVE-2024-9379, CVE-2024-8190, and CVE-2024-9380. Additionally, the Cybersecurity and Infrastructure Security Agency (CISA) has released a security advisory warning of threat actors leveraging these vulnerabilities in unison in active on-going campaigns.[1]

Title	CVE (CVSS 3.1)	Description	Affected products
Path Traversal in Ivanti CSA	CVE-2024-8963 (9.4)	Path Traversal in the Ivanti CSA allows a remote unauthenticated attacker to access restricted functionality.	Ivanti CSA before 4.6 Patch 519
OS Command Injection within Ivanti CSA	CVE-2024-8190 (7.2)	An OS command injection vulnerability allows a remote authenticated user (admin level) to obtain remote code execution.	Ivanti Cloud Services Appliance versions 4.6 Patch 518
OS Command Injection within Ivanti CSA	CVE-2024-9380 (7.2)	An OS command injection vulnerability in the admin web console of Ivanti CSA allows a remote authenticated user with admin	Ivanti CSA before version 5.0.2

		privileges to obtain remote code execution.	
SQL injection in Ivanti CSA	CVE-2024-9379 (7.2)	SQL injection in the admin web console of Ivanti CSA allows a remote authenticated user with admin privileges to run arbitrary SQL statements.	Ivanti CSA before version 5.0.2

Table 1[2,3,4,5]

The Cal-CSIC recommends immediately upgrading to Ivanti CSA 5.0.

For more information on applying the security updates please refer to the Ivanti's Security Advisory.

Organization, Source, Reference, and Dissemination Information

Organization Description	California Government Code § 8586.5 established the California Cybersecurity Integration Center (Cal-CSIC) as the central organizing hub of state government's cybersecurity activities, including information sharing, intelligence analysis, incident response, and overarching cybersecurity strategy. The Cal-CSIC is responsible for reducing the likelihood and severity of cyber incidents that could damage California's economy, critical infrastructure, and public or private sector networks in our state.
Customer Feedback	If you need further information about this issue, contact the Cal-CSIC at our email address CalCSIC@caloes.ca.gov or by telephone at (833) REPORT1.
Source Summary Statement	This report was compiled from a variety of sources, predominately open-source reporting.
Handling Caveats	**Traffic Light Protocol (TLP):** Recipients may share TLP:CLEAR information with the world; there is no limit on disclosure. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

[1] Cybersecurity and Infrastructure Security Agency; "Threat Actors Chained Vulnerabilities in Ivanti Cloud Service Applications"; https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-022a; accessed 7 February 2025.

[1] National Vulnerability Database; "CVE-2024-8963 Detail"; https://nvd.nist.gov/vuln/detail/CVE-2024-8963; accessed 7 February 2025.
[1] Ivanti; "Security Advisory Ivanti CSA 4.6 (Cloud Services Appliance) (CVE-2024-8963)"; https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-CSA-4-6-Cloud-Services-Appliance-CVE-2024-8963?language=en_US; accessed 7 February 2025.
[4] National Vulnerability Database; "CVE-2024-8190 Detail"; https://nvd.nist.gov/vuln/detail/CVE-2024-8190; accessed 7 February 2025.
[5] Ivanti; "Security Advisory Ivanti Cloud Service Appliance (CSA) (CVE-2024-8190)"; https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Cloud-Service-Appliance-CSA-CVE-2024-8190?language=en_US; accessed 7 February 2025.