CTI Evaluation Report

AA5-022A Threat Actors Chain Vulnerabilities In Ivanti Cloud Service Applications

Field	Value
Conversion type	STIX 2.1 → MISP
Conversion date	2025-10-09 14:05
Report generated	2026-06-30 06:30 UTC
UUID	`463a1e9c-b692-4d62-a6e8-cc61dbbc08f8`
Visibility	Public

> The Cybersecurity and Infrastructure Security Agency (CISA) and Federal Bureau of Investigation (FBI) are releasing this joint Cybersecurity Advisory in response to active exploitation of vulnerabilities in Ivanti Cloud Service Appliances (CSA): CVE-2024-8963, an administrative bypass vulnerability; CVE-2024-9379, a SQL injection vulnerability; and CVE-2024-8190 and CVE-2024-9380, remote code execution vulnerabilities.

According to CISA and trusted third-party incident response data, threat actors chained the listed vulnerabilities to gain initial access, conduct remote code execution (RCE), obtain credentials, and implant webshells on victim networks. The actors\u2019 primary exploit paths were two vulnerability chains. One exploit chain leveraged CVE-2024-8963 in conjunction with CVE-2024-8190 and CVE-2024-9380 and the other exploited CVE-2024-8963 and CVE-2024-9379. In one confirmed compromise, the actors moved laterally to two servers.

All four vulnerabilities affect Ivanti CSA version 4.6x versions before 519, and two of the vulnerabilities (CVE-2024-9379 and CVE-2024-9380) affect CSA versions 5.0.1 and below; according to Ivanti, these CVEs have not been exploited in version 5.0.

Ivanti CSA 4.6 is End-of-Life (EOL) and no longer receives patches or third-party libraries. CISA and FBI strongly encourage network administrators to upgrade to the latest supported version of Ivanti CSA. Network defenders are encouraged to hunt for malicious activity on their networks using the detection methods and indicators of compromise (IOCs) within this advisory. Credentials and sensitive data stored within the affected Ivanti appliances should

be considered compromised. Organizations should collect and analyze logs and artifacts for malicious activity and apply the incident response recommendations within this advisory.

Overall Score: ○ No data (N/A)

Community assessment based on **0 vote(s)** from the CTI-Transmute platform.

- **0 like(s)**

Methodology

Scores are derived from community votes on the **CTI-Transmute** platform using the MISP cti-evaluation taxonomy.

Level	Numeric score
very-low	0/100
low	25/100
moderate	50/100
high	75/100
very-high	100/100

The **overall score** is the mean of all dimension votes. The **consensus level** for a dimension requires at least 2 votes on the same level.

Generated by CTI-Transmute — 2026-06-30 06:30 UTC