CYBER ADVISORY

TLP:CLEAR

11 December 2024

Critical Ivanti Cloud Services Application Vulnerabilities

CVE-2024-11639 | CVE-2024-11772 | CVE-2024-11773 | Ivanti CSA

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of multiple vulnerabilities existing in Ivanti Cloud Services Application (CSA) versions prior to 5.0.3.[1] Ivanti CSA (Cloud Services Appliance) is a secure gateway solution that enables remote devices to connect to Ivanti Endpoint Manager (EPM) or Management Suite without requiring a traditional VPN.[2] The potential impact of exploitation is that an attacker could perform remote code execution on vulnerable versions. At present, there is no known exploit code publicly available, and no reported cases of this vulnerability being actively exploited.[3]

Affected Product	Issue	CVE (CVSS 3.1)
Ivanti Cloud Services Application 5.0.2 and prior	An authentication bypass in the admin web console of Ivanti CSA before 5.0.3 allows a remote unauthenticated attacker to gain administrative access	CVE-2024-11639 (10.0)
	Command injection in the admin web console of Ivanti CSA before version 5.0.3 allows a remote authenticated attacker with admin privileges to achieve remote code execution.	CVE-2024-11772 (9.1)
	SQL injection in the admin web console of Ivanti CSA before version 5.0.3 allows a remote authenticated attacker with admin privileges to run arbitrary SQL statements.	CVE-2024-11773 (9.1)

The Cal-CSIC recommends immediately updating to the latest Ivanti CSA version 5.0.3

For further information on applying updates please refer to Ivanti documentation.

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. To help us identify ways to better assist you, please submit feedback here.
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.
Information Needs	*HSEC 1.1; HSEC 1.2; HSEC 1.5; HSEC 1.8; HSEC 1.10; STAC KIQ 1.1; KIQ 1.2; KIQ 1.3; KIQ 1.4; KIQ 1.5*

[1] Bleeping Computer; "Ivanti warns of maximum severity CSA auth bypass vulnerability" https://www.bleepingcomputer.com/news/security/ivanti-warns-of-maximum-severity-csa-auth-bypass-vulnerability; accessed 11 December 2024

[2] Ivanti; "Configuring the Ivanti Cloud Services Appliance" https://help.ivanti.com/ld/help/en_US/LDMS/10.0/Windows/csa-h-help.htm#:~:text=The%20Ivanti%20Cloud%20Services%20Appliance%20(CSA)%20is%20an%20Internet%20appliance,proxy%20to%20access%20the%20Internet; accessed 11 December 2024

[3] Ivanti; "Security Advisory Ivanti Cloud Services Application (CSA) (CVE-2024-11639, CVE-2024-11772, CVE-2024-11773)" https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Cloud-Services-Application-CSA-CVE-2024-11639-CVE-2024-11772-CVE-2024-11773?language=en_US; accessed 11 December 2024