

CVE-2024-8190

Ivanti Cloud Services Appliance OS Command Injection Vulnerability

CISA KEV since Sep 13, 2024

Actively exploited

An OS command injection vulnerability in Ivanti Cloud Services Appliance versions 4.6 Patch 518 and before allows a remote authenticated attacker to obtain remote code execution. The attacker must have admin level privileges to exploit this vulnerability.

EVRS 81 /100 Urgent priority	CVSS V3.1 7.2 High · NVD	EPSS 0.885 99.78th percentile · FIRST	CISA DEADLINE Oct 4, 2024 KEV since 2024 · listed over a year
---	--	---	---

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.885 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.2	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: As Ivanti CSA has reached End-of-Life status, users are urged to remove CSA 4.6.x from service or upgrade to the 5.0.x line of supported solutions, as future vulnerabilities on the 4.6.x version of CSA are unlikely to receive future security updates.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
cloud services appliance	4.6	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-qjx2-rcx8-qr2r	Additional guidance	forums.ivanti.com/s/article/Security-Advisory-Ivanti-Cloud-Service-Appliance-CSA-CVE-2024-8190
NVD	nvd.nist.gov/vuln/detail/CVE-2024-8190	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2024-49004	Current data	evulnable.com/vulnerability-management/cve/CVE-2024-8190

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.