CVE-2024-8963

Ivanti Cloud Services Appliance (CSA) Path Traversal Vulnerability

Exigent | CISA KEV since Sep 19, 2024 | Actively exploited

Path Traversal in the Ivanti CSA before 4.6 Patch 519 allows a remote unauthenticated attacker to access restricted functionality.

EVRS	CVSS V3.1	EPSS	CISA DEADLINE
86/100 Immediate priority	9.1 Critical · NVD	0.986 99.92nd percentile · FIRST	Oct 10, 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	0.986 probability	− Pre-patch disclosure	Disclosure status unavailable
✓ CVSS	Base score 9.1	− Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent 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 security updates.

Basis: CISA KEV required action

Affected and fixed versions

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

Sources

Vendor guidance	github.com/advisories/GHSA-w7rx-cmpf-jrpp	Additional guidance	forums.ivanti.com/s/article/Security-Advisory-Ivanti-CSA-4-6-Cloud-Services-Appliance-CVE-2024-8963
NVD	nvd.nist.gov/vuln/detail/CVE-2024-8963	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2024-49510	Current data	evulnable.com/vulnerability-management/cve/CVE-2024-8963

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