

CVE-2024-50603

Aviatrix Controllers OS Command Injection Vulnerability

Exigent

CISA KEV since Jan 16, 2025

Actively exploited

An issue was discovered in Aviatrix Controller before 7.1.4191 and 7.2.x before 7.2.4996. Due to the improper neutralization of special elements used in an OS command, an unauthenticated attacker is able to execute arbitrary code. Shell metacharacters can be sent to /v1/api in cloud_type for list_flightpath_destination_instances, or src_cloud_type for flightpath_connection_test.

EVRS 88 /100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.985 99.92nd percentile · FIRST	CISA DEADLINE Feb 6, 2025 KEV since 2025 · 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	Added to CISA KEV within the last two years
☒ EPSS	0.985 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
controller	< 7.1.4191 ≥ 7.2 < 7.2.4996	7.1.4191 · 7.2.4996	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-2vqc-674h-xh9w	Additional guidance	docs.aviatrix.com/documentation/latest/release-notices/psirt-advisories/psirt-advisories.html?expand=true#remote-code-execution-vulnerability-in-aviatrix-controllers
docs.aviatrix.com	docs.aviatrix.com/documentation/latest/release-notices/psirt-advisories/psirt-advisories.html?expand=true	NVD	nvd.nist.gov/vuln/detail/CVE-2024-50603
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2024-44623
Current data	evulnable.com/vulnerability-management/cve/CVE-2024-50603		

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