

CVE-2021-40870

Aviatrix Controller Unrestricted Upload of File

Exigent

CISA KEV since Jan 18, 2022

Actively exploited

An issue was discovered in Aviatrix Controller 6.x before 6.5-1804.1922. Unrestricted upload of a file with a dangerous type is possible, which allows an unauthenticated user to execute arbitrary code via directory traversal.

EVRS 85 /100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.930 99.83rd percentile · FIRST	CISA DEADLINE Feb 1, 2022 KEV since 2022 · 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	0.930 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 updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
controller	≥ 6.2 < 6.2.2043 ≥ 6.3 < 6.3.2490 ≥ 6.4 < 6.4.2838 ≥ 6.5 < 6.5.1922	6.2.2043 · 6.3.2490 · 6.4.2838 · 6.5.1922	NVD

Sources

Vendor guidance github.com/advisories/GHSA-w7mg-q4hh-m9cq

Additional guidance docs.aviatrix.com/HowTos/UCC_Release_Notes.html#security-note-9-11-2021

NVD nvd.nist.gov/vuln/detail/CVE-2021-40870

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2021-28025

Current data evulnable.com/vulnerability-management/cve/CVE-2021-40870

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