

CVE-2025-66644

Array Networks ArrayOS AG OS Command Injection Vulnerability

CISA KEV since Dec 8, 2025

Actively exploited

Array Networks ArrayOS AG before 9.4.5.9 allows command injection, as exploited in the wild in August through December 2025.

EVRS 75 / ₁₀₀ Urgent priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.034 88.8th percentile · FIRST	CISA DEADLINE Dec 29, 2025 CISA federal deadline · Overdue by 10 months
--	--	--	---

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 year
☒ EPSS	0.034 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

Affected and fixed versions · 7 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
arrayos ag	< 9.4.5.9	9.4.5.9	NVD
ag1000	—	no fixed version listed	NVD
ag1000t	—	no fixed version listed	NVD
ag1000v5	—	no fixed version listed	NVD
ag1100	—	no fixed version listed	NVD
ag1100v5	—	no fixed version listed	NVD
ag1150	—	no fixed version listed	NVD
ag1200	—	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-hqfm-g725-ccqr	support.arraynetworks.net	support.arraynetworks.net/prx/001/http/supportportal.arraynetworks.net/ag.html
jpcert.or.jp	jpcert.or.jp/at/2025/at250024.html	NVD	nvd.nist.gov/vuln/detail/CVE-2025-66644
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2025-201500
Current data	evulnable.com/vulnerability-management/cve/CVE-2025-66644		

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