

CVE-2026-108456

Microsoft Azure AI Foundry Elevation of Privilege Vulnerability

Server-side request forgery (ssrf) in Azure AI Foundry allows an authorized attacker to elevate privileges over a network.

EVRS 12 /100 Elevated priority	CVSS V3.1 7.7 High · NVD	EPSS — Not scored	CISA DEADLINE — No CISA deadline
---	---------------------------------------	-------------------------	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 2 of 8 signals

☐ CISA KEV	Not currently CISA KEV-listed	☐ Vendor exploitation	Active-exploitation status not yet checked - scored at the population base rate (none) until known
☐ Ransomware	Ransomware association unavailable	☐ KEV recency	CISA KEV listing date unavailable
☐ EPSS	EPSS score not yet published - scored at FIRST's population median until known	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.7	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Scheduled Maintenance Untagged reference available; patch status is not confirmed

NVD lists one or more references for this CVE that aren't tagged as a patch or vendor advisory. Review them directly to confirm patch availability and applicability before making a remediation decision.

Basis: NVD reference (untagged)

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
Not identified by the connected sources	—	no fixed version listed	NVD

Sources

Reference	msrc.microsoft.com/update-guide/vulnerability/CVE-2026-108456	NVD	nvd.nist.gov/vuln/detail/CVE-2026-108456
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-108538	Current data	evulnable.com/vulnerability-management/cve/CVE-2026-108456

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