

CVE-2026-110063

Microsoft VM Inspector for Azure Virtual Machines Elevation of Privilege Vulnerability

Improper link resolution before file access ('link following') in VM Inspector for Azure Virtual Machines allows an unauthorized attacker to elevate privileges over a network.

EVRS 16 /100 Elevated priority	CVSS V3.1 10.0 Critical · NVD	EPSS 0.009 59.1st percentile · FIRST	CISA DEADLINE — No CISA deadline
---	---	--	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 3 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	0.009 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 10.0	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Scheduled Maintenance Patch or fixed version identified

Apply the vendor patch or guidance: <https://github.com/advisories/GHSA-pjxp-pqhh-mc2x> | <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-110063>

Basis: External remediation intelligence

Affected and fixed versions

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

Sources

Vendor guidance github.com/advisories/GHSA-pjxp-pqhh-mc2x

Additional guidance msrc.microsoft.com/update-guide/vulnerability/CVE-2026-110063

NVD nvd.nist.gov/vuln/detail/CVE-2026-110063

ENISA EUVD europa.eu/enisa/eu-vulnerability/EUVD-2026-108542

Current data evulnable.com/vulnerability-management/cve/CVE-2026-110063

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