

CVE-2026-118147

Microsoft Visual Studio Spoofing Vulnerability

Improper certificate validation in Visual Studio allows an unauthorized attacker to perform spoofing over a network.

EVRS 12 /100 Elevated priority	CVSS V3.1 7.4 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 7.4	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Scheduled Maintenance Patch or fixed version identified

Apply the vendor patch or guidance: <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-118147>

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	msrc.microsoft.com/update-guide/vulnerability/CVE-2026-118147	NVD	nvd.nist.gov/vuln/detail/CVE-2026-118147
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-114732	Current data	evulnable.com/vulnerability-management/cve/CVE-2026-118147

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