

CVE-2026-98318

Microsoft smb: client: validate absolute native symlink targets before NT fixups

In the Linux kernel, the following vulnerability has been resolved: smb: client: validate absolute native symlink targets before NT fixups With symlinkroot unset, an absolute target is copied without conversion to an NT drive path. Later code still assumes an NT prefix is present when modifying the target and calculating the print name length. For "/ab", this causes two failures: sym[5] and path[5] are written past their allocations, and plen -= 2 * poff subtracts an assumed 8-byte prefix from a 6-byte UTF-16

EVRS 12 /100 Elevated priority	CVSS V3.1 7.8 High · NVD	EPSS 0.001 2.3rd 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	0.001 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Scheduled Maintenance Patch or fixed version identified

Basis: External remediation intelligence

target, wrapping u16 plen to 65534. That underflow causes another overflow: memcpy() copies 65534 bytes into a 24-byte buffer. A user with write access to a mounted share can trigger these bugs with default settings. Validate the NT drive prefix, including an ASCII drive letter, before accessing fixed offsets or subtracting the prefix length.

Affected and fixed versions

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

Sources

Vendor guidance	git.kernel.org/stable/c/23c240d9509e15f72e4112fc95f0160ab32ec430	Additional guidance	git.kernel.org/stable/c/6913ff607c2bc8694193e1fcc40bf16d75f35f16
NVD	nvd.nist.gov/vuln/detail/CVE-2026-98318	ENISA EUVD	euid.europa.eu/vulnerability/EUVD-2026-93303
Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98318		

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