

CVE-2025-6218

RARLAB WinRAR Path Traversal Vulnerability

CISA KEV since Dec 9, 2025

Actively exploited

RARLAB WinRAR Directory Traversal Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of RARLAB WinRAR. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of file paths within archive files. A crafted file path can cause the process to traverse to unintended directories. An attacker can leverage this vulnerability to execute code in the context of the current user. Was ZDI-CAN-27198.

EVRS 85/100 Immediate priority	CVSS V3.0 7.8 High · NVD	EPSS 0.905 99.8th percentile · FIRST	CISA DEADLINE Dec 30, 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	0.905 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch Immediately 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

PACKAGE	AFFECTED	FIXED IN	SOURCE
winrar	< 7.12	7.12	NVD
windows	—	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-8x66-x5gf-2pc8	Additional guidance	win-rar.com/singlenewsview.html?&tx_ttnews%5Btt_news%5D=276&cHash=388885bd3908a40726f535c026f94eb6
win-rar.com	win-rar.com/singlenewsview.html?&L=0&tx_ttnews%5Btt_news%5D=276&cHash=b5165454d983fc9717bc8748901a64f9	NVD	nvd.nist.gov/vuln/detail/CVE-2025-6218
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2025-28706
Current data	evulnable.com/vulnerability-management/cve/CVE-2025-6218		

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