

CVE-2025-8088

RARLAB WinRAR Path Traversal Vulnerability

CISA KEV since Aug 12, 2025

Actively exploited

Ransomware use known

A path traversal vulnerability affecting the Windows version of WinRAR allows the attackers to execute arbitrary code by crafting malicious archive files. This vulnerability was exploited in the wild and was discovered by Anton Cherepanov, Peter Košinár, and Peter Strýček from ESET.

EVRS 91 /100 Immediate priority	CVSS V4.0 8.4 High · NVD	EPSS 0.945 99.86th percentile · FIRST	CISA DEADLINE Sep 2, 2025 KEV since 2025 · listed over a year
--	--	---	---

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	Known ransomware campaigns	☐ KEV recency	Added to CISA KEV within the last two years
☒ EPSS	0.945 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.4	☐ 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	< 7.13	no fixed version listed	NVD
dtsearch	< 2023.01	no fixed version listed	NVD
windows	—	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-832g-3rcm-wcrf

win-rar.com win-rar.com/singlenewsview.html?&L=0&tx_ttnews%5Btt_news%5D=283&cHash=a64b4a8f662d3639dec8d65f47bc93c5

NVD nvd.nist.gov/vuln/detail/CVE-2025-8088

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2025-23983

Current data evulnable.com/vulnerability-management/cve/CVE-2025-8088

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