

CVE-2023-38831

RARLAB WinRAR Code Execution Vulnerability

CISA KEV since Aug 24, 2023

Actively exploited

Ransomware use known

Public exploit module (Metasploit)

RARLAB WinRAR before 6.23 allows attackers to execute arbitrary code when a user attempts to view a benign file within a ZIP archive. The issue occurs because a ZIP archive may include a benign file (such as an ordinary .JPG file) and also a folder that has the same name as the benign file, and the contents of the folder (which may include executable content) are processed during an attempt to access only the benign file. This was exploited in the wild in April through October 2023.

EVRS 91/100 Immediate priority	CVSS V3.1 7.8 High · NVD	EPSS 0.998 99.96th percentile · FIRST	CISA DEADLINE Sep 14, 2023 KEV since 2023 · 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	On the CISA KEV catalog for over two years
☒ EPSS	0.998 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 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	< 6.23	6.23	NVD

Sources

Vendor guidance github.com/advisories/GHSA-w5x7-vwr2-4x27

win-rar.com win-rar.com/singlenewsview.html?&L=0&tx_ttnews%5Btt_news%5D=232&cHash=c5bf79590657e32554c6683296a8e8aa

NVD nvd.nist.gov/vuln/detail/CVE-2023-38831

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

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2023-42604

Current data evulnabile.com/vulnerability-management/cve/CVE-2023-38831

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