RARLAB WinRAR Code Execution Vulnerability

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2023-38831
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-08-23 17:15:00 UTC
Updated	2023-10-23 01:15:00 UTC
Description	RARLAB WinRAR before 6.23 allows attackers to execute arbitrary code when a user attempts to view a benign file within a

Risk And Classification

EPSS: 0.938780000 probability, percentile 0.998730000 (date 2026-04-22)

CISA KEV: Listed on 2023-08-24; due 2023-09-14; ransomware use Known

Problem Types: NVD-CWE-noinfo

CISA Known Exploited Vulnerability

Vendor	RARLAB
Product	WinRAR
Name	RARLAB WinRAR Code Execution Vulnerability
Required Action	Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.
Notes	http://www.win-rar.com/singlenewsview.html?&L=0&tx_ttnews%5Btt_news%5D=232&cHash=c5bf79590657e32554c6683296a8e8aa; https://nvd.nist.gov/vuln/detail/CVE-2023-38831

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Rarlab	Winrar	All	All	All	All

References

Reference	Source	Link	Tags
WinRAR zero-day exploited since April to hack trading accounts	MISC	www.bleepingcomputer.com	
WinRAR zero-day exploited since April to hack trading accounts | Hacker News	MISC	news.ycombinator.com	
Cybersecurity Services, Solutions & Products. Global Provider | Group-IB	MISC	www.group-ib.com	

Government-backed actors exploiting WinRAR vulnerability	MISC	blog.google	
WinRAR Remote Code Execution ≈ Packet Storm	MISC	packetstormsecurity.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, anal
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov	kev

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.