TOCTOU race in Linenoise enables arbitrary file overwrite and permission changes

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

Summary

CVE	CVE-2025-9810
State	PUBLISHED
Assigner	CyberArk
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-09-01 19:15:32 UTC
Updated	2026-04-22 16:16:52 UTC
Description	TOCTOU in linenoiseHistorySave in linenoise allows local attackers to overwrite arbitrary files and change permissions via

Risk And Classification

Primary CVSS: v3.1 5.8 MEDIUM from nvd@nist.gov

CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:H/A:L

EPSS: 0.000120000 probability, percentile 0.016060000 (date 2026-04-22)

Problem Types: CWE-367 | CWE-367 CWE-367 Time-of-check Time-of-use (TOCTOU) Race Condition

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	5.8	MEDIUM	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:H/A:L
3.1	96148269-fe82-4198-b1bf-3a73ce8bc92e	Secondary	6.8	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:L
3.1	CNA	CVSS	6.8	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:L

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

High

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

High

Availability

Low

CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:H/A:L

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Antirez	Linenoise	-	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Antirez	Linenoise	affected	Not specified

References

Reference	Source	Link
github.com/antirez/linenoise/commit/f2558e1e588b1ba384ec73a2cf5c9a464097...	af854a3a-2127-422b-91ae-364da2661108	github.com
github.com/antirez/linenoise/pull/202	96148269-fe82-4198-b1bf-3a73ce8bc92e	github.com
github.com/antirez/linenoise/blob/master/linenoise.c	96148269-fe82-4198-b1bf-3a73ce8bc92e	github.com
github.com/antirez/linenoise/blob/4111f1d6cd29e136b4e86a25d1dd859a1e0081...	af854a3a-2127-422b-91ae-364da2661108	github.com
CVE Program record	CVE.ORG	www.cve.or
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: @disconnect3d (en)

CNA: Simcha Kosman (en)

Additional Advisory Data

Solutions

CNA: call fchmod() on the fd instead of chmod() on the path

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report