



# TOCTOU race in Linenoise enables arbitrary file overwrite and permission changes

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2025-9810  |
| <b>State</b>           | PUBLISHED  |
| <b>Assigner</b>        | CyberArk   |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback   |
| <b>Published</b>       | 2025-09-01 19:15:32 UTC  |
| <b>Updated</b>         | 2026-04-22 16:16:52 UTC  |
| <b>Description</b>     | 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.o    |
| 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.

---

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)