



# Tabby: Unsafe protocol handler execution via terminal linkifier allows arbitrary OS protocol invocation

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

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2026-45037  |
| <b>State</b>           | PUBLISHED   |
| <b>Assigner</b>        | GitHub_M  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2026-05-15 17:16:48 UTC   |
| <b>Updated</b>         | 2026-05-15 17:16:48 UTC   |
| <b>Description</b>     | Tabby (formerly Terminus) is a highly configurable terminal emulator. Prior to 1.0.232, Tabby's terminal linkifier passes any |

## Risk And Classification

**Primary CVSS:** v3.1 7.1 HIGH from security-advisories@github.com

**CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L**

**Problem Types:** CWE-184 | CWE-601 | CWE-184 CWE-184: Incomplete List of Disallowed Inputs | CWE-601 CWE-601: URL Redirection to Untrusted Site ('Open Redirect')

| Version | Source                         | Type      | Score | Severity | Vector                                       |
|---------|--------------------------------|-----------|-------|----------|--|
| 3.1     | security-advisories@github.com | Secondary | 7.1   | HIGH     | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L |
| 3.1     | CNA                            | DECLARED  | 7.1   | HIGH     | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L |

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Changed

Confidentiality

Low

Integrity

Severity  
Low

Availability  
Low

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

---

Vendor Declared Affected Products

| Source | Vendor                  | Product               | Version            | Platforms     |
|--------|-------------------------|-----------------------|--------------------|---------------|
| CNA    | <a href="#">Eugeniy</a> | <a href="#">Tabby</a> | affected < 1.0.232 | Not specified |

---

References

| Reference   | Source   | Link  | Tags                |
|---|--|---|---------------------|
| <a href="https://github.com/Eugeniy/tabby/security/advisories/GHSA-cmpc-v2x9-j9x9">github.com/Eugeniy/tabby/security/advisories/GHSA-cmpc-v2x9-j9x9</a> | <a href="mailto:security-advisories@github.com">security-advisories@github.com</a> | <a href="https://github.com">github.com</a>     |                     |
| CVE Program record  | CVE.ORG  | <a href="https://www.cve.org">www.cve.org</a>   | canonical           |
| NVD vulnerability detail  | NVD  | <a href="https://nvd.nist.gov">nvd.nist.gov</a> | canonical, analysis |

---

No vendor comments have been submitted for this CVE.

---

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](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)