



# LinkAce: Password Reset Poisoning via X-Forwarded-Host Header Injection Leading to Account Takeover

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

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2026-40905  |
| <b>State</b>           | PUBLISHED   |
| <b>Assigner</b>        | GitHub_M  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2026-04-21 21:16:44 UTC   |
| <b>Updated</b>         | 2026-04-21 21:16:44 UTC   |
| <b>Description</b>     | LinkAce is a self-hosted archive to collect website links. Prior to 2.5.4, a password reset poisoning vulnerability was identified. |

## Risk And Classification

**Primary CVSS:** v3.1 8.1 HIGH from security-advisories@github.com

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

**Problem Types:** CWE-601 | CWE-601 CWE-601: URL Redirection to Untrusted Site ('Open Redirect')

| Version | Source                         | Type      | Score | Severity | Vector                                       |
|---------|--------------------------------|-----------|-------|----------|--|
| 3.1     | security-advisories@github.com | Secondary | 8.1   | HIGH     | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N |
| 3.1     | CNA                            | DECLARED  | 8.1   | HIGH     | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N |

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

None

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

### Vendor Declared Affected Products

| Source | Vendor                | Product                 | Version          | Platforms     |
|--------|-----------------------|-------------------------|------------------|---------------|
| CNA    | <a href="#">Kovah</a> | <a href="#">LinkAce</a> | affected < 2.5.4 | Not specified |

### References

| Reference   | Source   | Link  | Tags                |
|---|--|---|---------------------|
| <a href="https://github.com/Kovah/LinkAce/security/advisories/GHSA-48wv-jpf4-vjfv">github.com/Kovah/LinkAce/security/advisories/GHSA-48wv-jpf4-vjfv</a> | <a href="mailto:security-advisories@github.com">security-advisories@github.com</a> | <a href="https://github.com">github.com</a>     |                     |
| CVE Program record  | <a href="https://www.cve.org">CVE.ORG</a>  | <a href="https://www.cve.org">www.cve.org</a>   | canonical           |
| NVD vulnerability detail  | <a href="https://nvd.nist.gov">NVD</a>   | <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)