



# IRRD: web UI host header injection allows password reset poisoning via attacker-controlled email links

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

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2026-28681                               |
| <b>State</b>           | PUBLISHED                                    |
| <b>Assigner</b>        | GitHub_M                                     |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback |
| <b>Published</b>       | 2026-03-06 05:16:37 UTC                      |
| <b>Updated</b>         | 2026-04-21 14:45:02 UTC                      |

**Description** Internet Routing Registry daemon version 4 is an IRR database server, processing IRR objects in the RPSL format. From v

## 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-640 | CWE-601 CWE-601: URL Redirection to Untrusted Site ('Open Redirect') | CWE-640 CWE-640: Weak Password Recovery Mechanism for Forgotten Password

| 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

### NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor   | Product  | Version | Update | Edition | Language |
|-------------|--|--|---------|--------|---------|----------|
| Application | <a href="#">Internet Routing Registry Daemon Project</a> | <a href="#">Internet Routing Registry Daemon</a> | All     | All    | All     | All      |

### Vendor Declared Affected Products

| Source | Vendor                  | Product              | Version                    | Platforms     |
|--------|-------------------------|----------------------|----------------------------|---------------|
| CNA    | <a href="#">Irrdnet</a> | <a href="#">Irrd</a> | affected >= 4.4.0, < 4.4.5 | Not specified |
| CNA    | <a href="#">Irrdnet</a> | <a href="#">Irrd</a> | affected >= 4.5.0, < 4.5.1 | Not specified |

### References

| Reference   | Source   | Link  | Tag   |
|---|--|---|-------|
| <a href="https://github.com/irrdnet/irrd/commit/8408e0f1b9f47eb2f2e712d6153e32194df05fbb">github.com/irrdnet/irrd/commit/8408e0f1b9f47eb2f2e712d6153e32194df05fbb</a> | <a href="mailto:security-advisories@github.com">security-advisories@github.com</a> | <a href="https://github.com">github.com</a>                   | Patc  |
| <a href="https://irrd.readthedocs.io/en/stable/releases/4.4.5">irrd.readthedocs.io/en/stable/releases/4.4.5</a>   | <a href="mailto:security-advisories@github.com">security-advisories@github.com</a> | <a href="https://irrd.readthedocs.io">irrd.readthedocs.io</a> | Rele  |
| <a href="https://github.com/irrdnet/irrd/commit/cf62df4a49d3891e80b2879d9b324d1af050000c">github.com/irrdnet/irrd/commit/cf62df4a49d3891e80b2879d9b324d1af050000c</a> | <a href="mailto:security-advisories@github.com">security-advisories@github.com</a> | <a href="https://github.com">github.com</a>                   | Patc  |
| <a href="https://irrd.readthedocs.io/en/stable/releases/4.5.1">irrd.readthedocs.io/en/stable/releases/4.5.1</a>   | <a href="mailto:security-advisories@github.com">security-advisories@github.com</a> | <a href="https://irrd.readthedocs.io">irrd.readthedocs.io</a> | Rele  |
| <a href="https://github.com/irrdnet/irrd/security/advisories/GHSA-22m3-c7vp-49fj">github.com/irrdnet/irrd/security/advisories/GHSA-22m3-c7vp-49fj</a>                 | <a href="mailto:security-advisories@github.com">security-advisories@github.com</a> | <a href="https://github.com">github.com</a>                   | Mitig |
| CVE Program record  | CVE.ORG  | <a href="https://www.cve.org">www.cve.org</a>                 | canc  |
| NVD vulnerability detail  | NVD  | <a href="https://nvd.nist.gov">nvd.nist.gov</a>               | canc  |

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)