



# Spinnaker clouddriver and orca URL validation bypass via underscores in hostnames

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

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2026-25534  |
| <b>State</b>           | PUBLISHED   |
| <b>Assigner</b>        | GitHub_M  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2026-03-17 18:16:15 UTC   |
| <b>Updated</b>         | 2026-04-16 14:46:24 UTC   |
| <b>Description</b>     | ### Impact Spinnaker updated URL Validation logic on user input to provide sanitation on user inputted URLs for clouddriver |

## Risk And Classification

**Primary CVSS:** v3.1 9.1 CRITICAL from security-advisories@github.com

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

**EPSS:** 0.000460000 probability, percentile 0.140390000 (date 2026-04-16)

**Problem Types:** CWE-918 | CWE-918 CWE-918: Server-Side Request Forgery (SSRF)

| Version | Source                         | Type      | Score | Severity | Vector                                       |
|---------|--------------------------------|-----------|-------|----------|--|
| 3.1     | security-advisories@github.com | Secondary | 9.1   | CRITICAL | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:L |
| 3.1     | CNA                            | DECLARED  | 9.1   | CRITICAL | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:L |

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Changed

Confidentiality

High

Integrity

Low

Availability

Low

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

### Vendor Declared Affected Products

| Source | Vendor                                   | Product                               | Version                          | Platforms     |
|--------|--|---------------------------------------|----------------------------------|---------------|
| CNA    | <a href="#">lo.spinnaker.clouddriver</a> | <a href="#">Clouddriver-artifacts</a> | affected < 2025.2.4              | Not specified |
| CNA    | <a href="#">lo.spinnaker.clouddriver</a> | <a href="#">Clouddriver-artifacts</a> | affected >= 2025.3.0, < 2025.3.1 | Not specified |
| CNA    | <a href="#">lo.spinnaker.clouddriver</a> | <a href="#">Clouddriver-artifacts</a> | affected >= 2025.4.0, < 2025.4.1 | Not specified |
| CNA    | <a href="#">lo.spinnaker.orca</a>        | <a href="#">Orca-core</a>             | affected < 2025.2.4              | Not specified |
| CNA    | <a href="#">lo.spinnaker.orca</a>        | <a href="#">Orca-core</a>             | affected >= 2025.3.0, < 2025.3.1 | Not specified |
| CNA    | <a href="#">lo.spinnaker.orca</a>        | <a href="#">Orca-core</a>             | affected >= 2025.4.0, < 2025.4.1 | Not specified |

### References

| Reference   | Source   | Link                         | Tag |
|---|--|------------------------------|-----|
| <a href="#">github.com/spinnaker/spinnaker/security/advisories/GHSA-8r8j-gfhg-fw38</a>      | <a href="#">security-advisories@github.com</a> | <a href="#">github.com</a>   |     |
| <a href="#">github.com/spinnaker/spinnaker/security/advisories/GHSA-vrjc-q2fh-6x9h</a>      | <a href="#">security-advisories@github.com</a> | <a href="#">github.com</a>   |     |
| <a href="#">github.com/spinnaker/spinnaker/commit/7c4737906239a958a468e843239c6785b0...</a> | <a href="#">security-advisories@github.com</a> | <a href="#">github.com</a>   |     |
| CVE Program record  | CVE.ORG  | <a href="#">www.cve.org</a>  | can |
| NVD vulnerability detail  | NVD  | <a href="#">nvd.nist.gov</a> | can |

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](#)

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