



# Pi-hole: Local privilege escalation via config-controlled path in root-executed service hooks

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

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2026-41489  |
| <b>State</b>           | PUBLISHED   |
| <b>Assigner</b>        | GitHub_M  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2026-05-11 21:19:00 UTC   |
| <b>Updated</b>         | 2026-05-12 16:38:54 UTC   |
| <b>Description</b>     | Pi-hole is a DNS sinkhole that protects devices from unwanted content without installing any client-side software. From 6.0 |

## Risk And Classification

**Primary CVSS:** v3.1 8.8 HIGH from security-advisories@github.com

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

**EPSS:** 0.000120000 probability, percentile 0.017080000 (date 2026-05-12)

**Problem Types:** CWE-15 | CWE-269 | CWE-732 | CWE-732 CWE-732: Incorrect Permission Assignment for Critical Resource | CWE-269 CWE-269: Improper Privilege Management | CWE-15 CWE-15: External Control of System or Configuration Setting

| Version | Source                         | Type      | Score | Severity | Vector                                       |
|---------|--------------------------------|-----------|-------|----------|--|
| 3.1     | security-advisories@github.com | Secondary | 8.8   | HIGH     | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H |
| 3.1     | CNA                            | DECLARED  | 8.8   | HIGH     | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H |

## CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Changed

Confidentiality

High

Integrity

High

Availability

High

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

### Vendor Declared Affected Products

| Source | Vendor  | Product | Version                  | Platforms     |
|--------|---------|---------|--------------------------|---------------|
| CNA    | Pi-hole | Pi-hole | affected >= 6.0, < 6.4.2 | Not specified |

### References

| Reference  | Source                         | Link         | Tags                |
|--|--------------------------------|--------------|---------------------|
| github.com/pi-hole/pi-hole/security/advisories/GHSA-6w8x-p785-6pm4 | security-advisories@github.com | github.com   |                     |
| CVE Program record   | CVE.ORG                        | www.cve.org  | canonical           |
| NVD vulnerability detail   | NVD                            | nvd.nist.gov | 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)