



# Nhost Leaks the Refresh Token via URL Query Parameter in OAuth Provider Callback

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

## Summary

<b>CVE</b>	CVE-2026-34969
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitHub_M
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-06 16:16:38 UTC
<b>Updated</b>	2026-04-06 16:16:38 UTC
<b>Description</b>	Nhost is an open source Firebase alternative with GraphQL. Prior to 0.48.0, the auth service's OAuth provider callback flow

## Risk And Classification

**Primary CVSS:** v4.0 2.3 LOW from security-advisories@github.com

CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:P/VC:N/VI:N/VA:N/SC:L/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**Problem Types:** CWE-200 | CWE-598 | CWE-200 CWE-200: Exposure of Sensitive Information to an Unauthorized Actor | CWE-598 CWE-598: Use of GET Request Method With Sensitive Query Strings

Version	Source	Type	Score	Severity	Vector
4.0	security-advisories@github.com	Secondary	2.3	LOW	CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:P/VC:N/VI:N/VA:N/SC:L/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
4.0	CNA	DECLARED	2.3	LOW	CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:P/VC:N/VI:N/VA:N/SC:L/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Attack Requirements

Present

Privileges Required

None

User Interaction

Passive

Confidentiality

None

Integrity

None

Availability

None

Sub Conf.

Low

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:P/VC:N/VI:N/VA:N/SC:L/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Nhost	Nhost	affected < 0.48.0	Not specified

### References

Reference	Source	Link	Tags
github.com/nhost/nhost/security/advisories/GHSA-g2qj-prgh-4g9r	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.

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