



zrok: WebDAV drive backend follows symlinks outside DriveRoot, enabling host filesystem read/write

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

Summary

CVE	CVE-2026-42275
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-08 04:16:22 UTC
Updated	2026-05-08 04:16:22 UTC
Description	zrok is software for sharing web services, files, and network resources. Prior to version 2.0.2, the zrok WebDAV drive backe

Risk And Classification

Primary CVSS: v3.1 8.7 HIGH from security-advisories@github.com

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

Problem Types: CWE-22 | CWE-61 | CWE-61 CWE-61: UNIX Symbolic Link (Symlink) Following | CWE-22 CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	8.7	HIGH	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:N
3.1	CNA	DECLARED	8.7	HIGH	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Changed

Confidentiality

High

Integrity

High

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Openziti	Zrok	affected < 2.0.2	Not specified

References

Reference	Source	Link	Tags
github.com/openziti/zrok/commit/459bcfc1e121decae1b1d11c37ad94e4ed5bbf2e	security-advisories@github.com	github.com	
github.com/openziti/zrok/security/advisories/GHSA-74m3-9qvm-rp9h	security-advisories@github.com	github.com	
github.com/openziti/zrok/releases/tag/v2.0.2	security-advisories@github.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

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