



External Secrets Operator has DNS exfiltration via getHostByName in its v2 template engine

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

Summary

CVE	CVE-2026-34984
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-14 03:16:08 UTC
Updated	2026-04-17 15:26:13 UTC
Description	External Secrets Operator reads information from a third-party service and automatically injects the values as Kubernetes S

Risk And Classification

Primary CVSS: v4.0 7.1 HIGH from security-advisories@github.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/VA:N/SC:N/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

EPSS: 0.000440000 probability, percentile 0.133520000 (date 2026-04-20)

Problem Types: CWE-200 | CWE-200 CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Version	Source	Type	Score	Severity	Vector
4.0	security-advisories@github.com	Secondary	7.1	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/VA:N/SC:N/S
4.0	CNA	DECLARED	7.1	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/VA:N/SC:N/S

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

None

Confidentiality: **High**

Integrity: **None**

Availability: **None**

Sub Conf.: **None**

Sub Integrity: **None**

Sub Availability: **None**

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/VA:N/SC:N/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	External-secrets	External-secrets	affected < 2.3.0	Not specified

References				
Reference	Source	Link	Tags	
github.com/external-secrets/external-secrets/releases/tag/v2.3.0	security-advisories@github.com	github.com		
github.com/external-secrets/external-secrets/commit/6800989bdc12782ca260...	security-advisories@github.com	github.com		
github.com/external-secrets/external-secrets/security/advisories/GHSA-r2...	security-advisories@github.com	github.com		
CVE Program record	CVE.ORG	www.cve.org	canonica	
NVD vulnerability detail	NVD	nvd.nist.gov	canonica	

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

