



Helm has a path traversal in plugin metadata version enables arbitrary file write outside Helm plugin directory

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

Summary

CVE	CVE-2026-35204
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-09 16:16:27 UTC
Updated	2026-04-17 14:07:05 UTC
Description	Helm is a package manager for Charts for Kubernetes. From 4.0.0 to 4.1.3, a specially crafted Helm plugin, when installed

Risk And Classification

Primary CVSS: v4.0 8.4 HIGH from security-advisories@github.com

CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:P/VC:N/VI:H/VA:L/SC:H/SI:H/SA:H/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: 0.000120000 probability, percentile 0.017420000 (date 2026-04-21)

Problem Types: CWE-22 | CWE-22 CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Version	Source	Type	Score	Severity	Vector
4.0	security-advisories@github.com	Secondary	8.4	HIGH	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:P/VC:N/VI:H/VA:L/SC:H/SI:H/SA:H/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	8.4	HIGH	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:P/VC:N/VI:H/VA:L/SC:H/SI:H/SA:H/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
3.1	nvd@nist.gov	Primary	8.6	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:C/H/I:H/A:H

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

Passive

Confidentiality

None

Integrity

High

Availability

Low

Sub Conf.

High

Sub Integrity

High

Sub Availability

High

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

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Changed

Confidentiality

High

Integrity

High

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Helm	Helm	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
--------	--------	---------	---------	-----------

Source	Vendor	Product	Version	Platform
CNA	Helm	Helm	affected >= 4.0.0, < 4.1.4	Not specified

References

Reference	Source	Link	Tags
github.com/helm/helm/releases/tag/v4.1.4	security-advisories@github.com	github.com	Product,
github.com/helm/helm/security/advisories/GHSA-vmx8-mqv2-9gmg	security-advisories@github.com	github.com	Mitigation
github.com/helm/helm/commit/36c8539e99bc42d7aef9b87d136254662d04f027	security-advisories@github.com	github.com	Patch
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.cve.org). 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