Hackage package metadata stored XSS vulnerability

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-40472
State	PUBLISHED
Assigner	redhat-cnalr
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-23 16:16:25 UTC
Updated	2026-04-24 14:41:55 UTC
Description	In hackage-server, user-controlled metadata from .cabal files are rendered into HTML href attributes without proper sanitiza

Risk And Classification

Primary CVSS: v3.1 9.9 CRITICAL from 74b3a70d-cca6-4d34-9789-e83b222ae3be

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

EPSS: 0.000460000 probability, percentile 0.141240000 (date 2026-04-24)

Problem Types: CWE-79 | CWE-79 CWE-79 Improper neutralization of input during web page generation ('cross-site scripting')

Version	Source	Type	Score	Severity	Vector
3.1	74b3a70d-cca6-4d34-9789-e83b222ae3be	Secondary	9.9	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:L
3.1	CNA	CVSS	9.9	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:L

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Changed

Confidentiality

High

ntegrity

High

Availability

Low

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

There are no known software configurations currently associated with this CVE in NVD or the CVE Program record.

References

Reference	Source	Link	Tags
osv.dev/vulnerability/HSEC-2026-0004	74b3a70d-cca6-4d34-9789-e83b222ae3be	osv.dev	
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.