Zip Slip Path Traversal on Node Unpack

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

Summary

CVE	CVE-2026-2741
State	PUBLISHED
Assigner	Vaadin
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-10 18:18:48 UTC
Updated	2026-05-07 18:44:38 UTC
Description	Specially crafted ZIP archives can escape the intended extraction directory during Node.js download and extraction in Vaac

Risk And Classification

Primary CVSS: v4.0 2.3 LOW from security@vaadin.com

CVSS:4.0/AV:N/AC:H/AT:P/PR:L/UI:N/VC:L/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/MSC:X/MSI:X/MSA:X/S:N/AU:N/R:U/V:D/RE:L/U:Amber

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@vaadin.com	Secondary	2.3	LOW	CVSS:4.0/AV:N/AC:H/AT:P/PR:L/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N/E:X
4.0	CNA	CVSS	2.3	LOW	CVSS:4.0/AV:N/AC:H/AT:P/PR:L/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N/S:N
3.1	nvd@nist.gov	Primary	6.8	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:H/A:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Attack Requirements

Present

Privileges Required

Low

User Interaction

None

Confidentiality

Low

Integrity

None

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:H/AT:P/PR:L/UI:N/VC:L/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/MSC:X/MSI:X/MSA:X/S:N/AU:N/R:U/V:D/RE:L/U:Amber

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Changed

Confidentiality

None

Integrity

High

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms

CNA	Vaadin	Vaadin	affected 14.2.0 14.14.0 maven	Not specified
CNA	Vaadin	Vaadin	affected 15.0.0 23.6.6 maven	Not specified
CNA	Vaadin	Vaadin	affected 24.0.0 24.9.8 maven	Not specified
CNA	Vaadin	Vaadin	affected 25.0.0 25.0.2 maven	Not specified
CNA	Vaadin	Flow	affected 2.2.0 2.13.0 maven	Not specified
CNA	Vaadin	Flow	affected 3.0.0 23.6.7 maven	Not specified
CNA	Vaadin	Flow	affected 24.0.0 24.9.9 maven	Not specified
CNA	Vaadin	Flow	affected 25.0.0 25.0.3 maven	Not specified

References

Reference	Source	Link	Tags
github.com/vaadin/flow/pull/23133	security@vaadin.com	github.com	Issue Tracking, Patch
github.com/vaadin/flow/pull/23131	security@vaadin.com	github.com	Issue Tracking, Patch
github.com/vaadin/flow/pull/23125	security@vaadin.com	github.com	Issue Tracking, Patch
github.com/vaadin/flow/pull/23130	security@vaadin.com	github.com	Issue Tracking, Patch
vaadin.com/security/cve-2026-2741	security@vaadin.com	vaadin.com	Vendor Advisory
github.com/vaadin/flow/pull/23135	security@vaadin.com	github.com	Issue Tracking, Patch
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.

Additional Advisory Data

Solutions

CNA: Users of affected versions should apply the following mitigation or upgrade.

Workarounds

CNA: Use a globally preinstalled Node.js that is compatible with the Vaadin version instead of relying on Vaadin's automatic Node.js download.

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

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**