Apache Camel Platform HTTP Main: Authentication Bypass on Non-Root Context Paths in camel main runtime

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

Summary

CVE	CVE-2026-40022
State	PUBLISHED
Assigner	apache
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-27 10:16:09 UTC
Updated	2026-04-27 10:16:09 UTC
Description	When authentication is enabled on the Apache Camel embedded HTTP server or embedded management server (camel-p

Risk And Classification

Problem Types: CWE-288 | CWE-288 CWE-288 Authentication Bypass Using an Alternate Path or Channel

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Apache Software Foundation	Apache Camel Platform HTTP Main	affected 4.14.1 4.14.6 semver	Not specified
CNA	Apache Software Foundation	Apache Camel Platform HTTP Main	affected 4.18.0 4.18.2 semver	Not specified

References

Reference	Source	Link	Tags
camel.apache.org/security/CVE-2026-40022.html	security@apache.org	camel.apache.org	
www.openwall.com/lists/oss-security/2026/04/26/5	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Jihang Yu (en)

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**