APACHE CAMEL SECURITY ADVISORY: CVE-2026-40022

Search

SEVERITY

MEDIUM

SUMMARY

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

VERSIONS AFFECTED

From 4.14.1 before 4.14.6, from 4.15.0 before 4.18.2.

VERSIONS FIXED

4.14.6, 4.18.2 and 4.20.0

DESCRIPTION

When authentication is enabled on the Apache Camel embedded HTTP server or embedded management server (camel-platform-http-main) and a non-root context path such as /api or /admin is configured via camel.server.path or camel.management.path, the BasicAuthenticationConfigurer and JWTAuthenticationConfigurer classes derive the authentication path from properties.getPath() when camel.server.authenticationPath / camel.management.authenticationPath is not explicitly set. Combined with the Vert.x sub-router mounting model — the sub-router is mounted at _path_* and the authentication handler is registered inside the sub-router at the resolved path — this causes the authentication handler to match only the exact configured context path, not its subpaths. Unauthenticated requests to subpaths such as /api/_route_ or /admin/observe/info therefore reach protected business routes and management endpoints without being challenged for credentials. The /observe/info endpoint can disclose runtime metadata such as the user, working directory, home directory, process ID, JVM and operating system information.

NOTES

The pull requests https://github.com/apache/camel/pull/22474 (main), https://github.com/apache/camel/pull/22475 (4.18.x) and https://github.com/apache/camel/pull/22476 (4.14.x) refer to the commits that resolved the issue, and have more details.

MITIGATION

Users are recommended to upgrade to version 4.20.0, which fixes the issue. If users are on the 4.14.x LTS releases stream, they are suggested to upgrade to 4.14.6. If users are on the 4.18.x LTS releases stream, they are suggested to upgrade to 4.18.2.

CREDIT

This issue was discovered by Jihang Yu

REFERENCES

PGP signed advisory data: CVE-2026-40022.txt.asc
Mitre CVE Entry: https://www.cve.org/CVERecord?id=CVE-2026-40022

Edit this Page Back to top

Overview

Blog
Documentation
Community
Download

Documentation

User Manual
Components
Camel-K
Camel Kafka Connector
Camel Quarkus
Camel Spring Boot
Camel Karaf
FAQ

Community

Support
Contributing
Mailing Lists
User stories
Articles
Books
Team

About

Acknowledgments
Apache Events
License
Security
Sponsorship
Thanks

PRIVACY POLICY • CODE OF CONDUCT • SITEMAP