NATIONAL CSIRT-CY

CVE-2025-29891 **13/3/2025**

Camel Message Header Injection through request parameters

Executive Summary

This vulnerability is present in Camel's default incoming header filter, that allows an attacker to include Camel specific headers that for some Camel components can alter the behaviours such as the camel-bean component, or the camel-exec component.

Analysis

If you have Camel applications that are directly connected to the internet via HTTP, then an attacker could include parameters in the HTTP requests that are sent to the Camel application that incorrectly get translated into headers. The headers could be both provided as request parameters for an HTTP methods invocation or as part of the payload of the HTTP methods invocation. All the known Camel HTTP component such as camel-servlet, camel-jetty, camel-undertow, camel-platform-http, and camel-netty-http would be vulnerable out of the box.

Common Weakness Enumeration

https://cwe.mitre.org/data/definitions/164.html

Common Vulnerabilities & Exposures

https://nvd.nist.gov/vuln/detail/CVE-2025-29891

Versions affected

Apache Camel 4.10.0 before 4.10.2.

Apache Camel 4.8.0 before 4.8.5.

Apache Camel 3.10.0 before 3.22.4.

Solutions

Users are recommended to upgrade to version 4.10.2 for 4.10.x LTS, 4.8.5 for 4.8.x LTS and 3.22.4 for 3.x releases. Also, users could use removeHeaders EIP, to filter out anything like ‘cAmel, cAMEL’ etc, or in general everything not starting with ‘Camel’, ‘camel’ or ‘org.apache.camel.’.

Versions fixed

3.22.4, 4.8.5 and 4.10.2

Please distribute this information among your subsidiaries and partners, and also share with us any pertinent information and findings you may have (e.g IOCs, TTPs etc)

The Digital Security Authority extends its appreciation for the continued collaboration.

Disclaimer

Organizations are advised to consult with relevant cybersecurity professionals and follow best practices for their specific environments.