APACHE CAMEL SECURITY ADVISORY: CVE-2026-40453

Search

SEVERITY

Medium

SUMMARY

Incomplete fix for CVE-2025-27636 in non-HTTP HeaderFilterStrategies (camel-jms, camel-sjms, camel-coap, camel-google-pubsub) allows case-variant header injection

VERSIONS AFFECTED

From 3.0.0 before 4.14.6, from 4.15.0 before 4.18.2, from 4.19.0 before 4.20.0.

VERSIONS FIXED

4.14.6, 4.18.2 and 4.20.0

DESCRIPTION

The fix for CVE-2025-27636 added setLowerCase(true) to HttpHeaderFilterStrategy so that case-variant header names such as 'CAmelExecCommandExecutable' are filtered out alongside 'CamelExecCommandExecutable'. The same setLowerCase(true) call was not applied to five non-HTTP HeaderFilterStrategy implementations: JmsHeaderFilterStrategy and ClassicJmsHeaderFilterStrategy in camel-jms, SjmsHeaderFilterStrategy in camel-sjms, CoAPHeaderFilterStrategy in camel-coap, and GooglePubsubHeaderFilterStrategy in camel-google-pubsub. Because those strategies use case-sensitive String.startsWith('Camel'/'camel') filtering while the Camel Exchange stores headers in a case-insensitive map, an attacker with JMS (or equivalent) producer access to the broker consumed by a Camel route can inject case-variant Camel internal headers, which are then resolved by downstream components such as camel-exec and camel-file using their canonical casing. This enables remote code execution and arbitrary file write on routes that forward JMS messages to header-driven components.

NOTES

The JIRA ticket: https://issues.apache.org/jira/browse/CAMEL-23313 refers to the various commits that resolved the issue, and have more details. This advisory completes the fix for CVE-2025-27636 by extending setLowerCase(true) to the non-HTTP HeaderFilterStrategy implementations that were not updated in the original 2025-03-09 advisory.

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, then they are suggested to upgrade to 4.14.6. If users are on the 4.18.x releases stream, then they are suggested to upgrade to 4.18.2.

CREDIT

This issue was discovered by Saroj Khadka

REFERENCES

PGP signed advisory data: CVE-2026-40453.txt.asc
Mitre CVE Entry: https://www.cve.org/CVERecord?id=CVE-2026-40453

Edit this Page Back to top