APACHE CAMEL SECURITY ADVISORY: CVE-2026-40048

Search

SEVERITY

HIGH

SUMMARY

Camel-PQC: Unsafe Deserialization from FileBasedKeyLifecycleManager

VERSIONS AFFECTED

From 4.19.0 before 4.20.0, from 4.18.0 before 4.18.2.

VERSIONS FIXED

4.18.2 and 4.20.0

DESCRIPTION

The Camel-PQC FileBasedKeyLifecycleManager class deserializes the contents of `<keyId>.key` files in the configured key directory using java.io.ObjectInputStream without applying any ObjectInputFilter or class-loading restrictions. The cast to `java.security.KeyPair` is evaluated only after `readObject()` has already returned, so any `readObject()` side effects in the deserialized object run before the type check. An attacker who can write to the key directory used by a Camel application — for example through a path traversal into the directory, misconfigured filesystem permissions on the volume where keys are stored, a compromised key provisioning pipeline, or a symlink attack — can place a crafted serialized Java object that, when deserialized during normal key lifecycle operations, results in arbitrary code execution in the context of the application.

NOTES

The JIRA ticket: https://issues.apache.org/jira/browse/CAMEL-23200 refers to the various commits that resolved the issue, and have more details.

MITIGATION

Users are recommended to upgrade to version 4.20.0, which fixes the issue by replacing java.io.ObjectInputStream-based key and metadata storage with standard PKCS#8 (private key) / X.509 SubjectPublicKeyInfo (public key) Base64 JSON encoding. For users on the 4.18.x LTS releases stream, upgrade to 4.18.2.

CREDIT

This issue was discovered by Andrea Cosentino from Apache Software Foundation and Venkatraman Kumar from Securin

REFERENCES

PGP signed advisory data: CVE-2026-40048.txt.asc

Mitre CVE Entry: https://www.cve.org/CVERecord?id=CVE-2026-40048

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