



## APACHE CAMEL SECURITY ADVISORY · CVE-2026-27172

Q Search

### SEVERITY

High

### SUMMARY

Apache Camel: Unsafe Java deserialization in camel-consul ConsulRegistry allows arbitrary code execution via malicious values read from the Consul KV store

### VERSIONS AFFECTED

From 3.0.0 before 4.14.6 and from 4.15.0 before 4.18.1

### VERSIONS FIXED

4.14.6, 4.18.1 and 4.19.0

### DESCRIPTION

The ConsulRegistry in the camel-consul component (class `org.apache.camel.component.consul.ConsulRegistry` and its inner `ConsulRegistryUtils.deserialize` method) read Java-serialized values from the Consul KV store and passed them to `ObjectInputStream.readObject()` without configuring an `ObjectInputFilter`. An attacker who can write to the Consul KV store backing a Camel ConsulRegistry instance could inject a malicious serialized Java object that is deserialized the next time Camel performs a lookup against that registry, leading to arbitrary code execution in the Camel process. The issue mirrors the class of vulnerability already addressed for other Camel components in CVE-2024-22369, CVE-2024-23114 and CVE-2026-25747, and was overlooked during the original remediation of those CVEs.

### NOTES

The JIRA ticket: <https://issues.apache.org/jira/browse/CAMEL-23029> refers to the commits that resolved the issue and has more details. The vulnerability is of the same class as CVE-2024-22369, CVE-2024-23114 and CVE-2026-25747: a Camel component reads Java-serialized bytes from a backing store and passes them to `ObjectInputStream.readObject()` without any class allowlist, so an attacker who can influence the bytes in that store can trigger arbitrary code execution via a gadget chain. In camel-consul, the affected path is `ConsulRegistry.lookupByName` (and transitively `lookupByNameAndType`, `findByTypeWithName` and `findByType`), which reads a Base64-encoded Java-serialized object from the Consul key/value store and deserializes it.

### MITIGATION

Users are recommended to upgrade to version 4.19.0, 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 4.18.1.

### CREDIT

This issue was discovered and fixed by Andrea Cosentino of Apache Software Foundation

### REFERENCES

PGP signed advisory data: [CVE-2026-27172.txt.asc](#)

Mitre CVE Entry: <https://www.cve.org/CVERecord?id=CVE-2026-27172>

[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](#)

© 2004-2026 The [Apache Software Foundation](#).

Apache Camel, Camel, Apache, the Apache feather logo, and the Apache Camel project logo are trademarks of The Apache Software Foundation. All other marks mentioned may be trademarks or registered trademarks of their respective owners.

[PRIVACY POLICY](#) ● [CODE OF CONDUCT](#) ● [SITEMAP](#)

