مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerability in Apache Camel

Tracking #:432316983

Date:18-03-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in **Apache Camel**, a widely-used open-source integration framework. This vulnerability, which impacts several HTTP components, can potentially allow attackers to inject malicious headers into applications, compromising their behavior and functionality.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2025-29891**
- A high-severity vulnerability exists in Apache Camel. This flaw allows attackers to inject malicious headers via HTTP request parameters, potentially manipulating application behavior. The vulnerability resides in Camel's default incoming header filter, enabling attackers to inject Camel-specific headers that can alter the behavior of components like camel-bean and camel-exec. This is particularly concerning for applications directly exposed to the internet via HTTP.
- Successful exploitation of this vulnerability could lead to:
  - Arbitrary code execution through vulnerable components.
  - Manipulation of application logic and data flow.
  - Unauthorized access to sensitive information.
  - Denial of service.
- A proof-of-concept (PoC) exploit is available for CVE-2025-29891, emphasizing the severity of this issue.

Affected Components:

- camel-servlet
- camel-jetty
- camel-undertow
- camel-platform-http
- camel-netty-http

Affected Versions:

- Apache Camel 4.10.0 to 4.10.1
- Apache Camel 4.8.0 to 4.8.4
- Apache Camel 3.10.0 to 3.22.3

Fixed Versions:

- Apache Camel 3.22.4
- Apache Camel 4.8.5
- Apache Camel 4.10.2

RECOMMENDATIONS:

- **Upgrade to Patched Versions:**
  - Upgrade to the patched versions (3.22.4, 4.8.5, or 4.10.2) as recommended by the Apache Software Foundation.

- **Additional Header Filtering:**
  - Implement the **RemoveHeaders Enterprise Integration Pattern (EIP)** to filter out potentially malicious headers.
  - Specifically, filter out any headers containing 'cAmel' or 'cAMEL', or any headers not starting with 'Camel', 'camel', or 'org.apache.camel'.
- **Monitor and Review Logs:**
  - Continuously monitor your application's HTTP request logs for any signs of suspicious activity that could indicate exploitation attempts.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://camel.apache.org/security/CVE-2025-29891.html
- https://github.com/akamai/CVE-2025-27636-Apache-Camel-PoC