



NCSC-2026-0129

Kwetsbaarheden verholpen in Apache Camel

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 29-04-2026

TLP:WHITE

Toegestane verspreiding van TLP:WHITE

(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

Apache Software Foundation heeft kwetsbaarheden verholpen in Apache Camel.

Duiding

De kwetsbaarheden bevinden zich in verschillende componenten van Apache Camel. De problemen betreffen onder andere onveilige deserialisatie, onvoldoende filtering van e-mailheaders, onjuiste authenticatiepadmatching, en onjuiste verwerking van interne headers. De meest ernstige kwetsbaarheid stelt kwaadwillenden in staat om ongeauthenticeerd op afstand willekeurige code uit te voeren. De kwetsbaarheden zijn aanwezig in diverse versies van Apache Camel, met name vanaf versie 3.0.0 tot net voor de gepatchte versies 4.14.6, 4.14.7, 4.18.1, 4.18.2, 4.19.0 en 4.20.0, afhankelijk van de component. De fixes omvatten onder meer het toepassen van veilige deserialisatie, correcte filtering van headers, en verbeterde authenticatiecontroles.

Oplossingen

Apache Software Foundation heeft updates uitgebracht in Apache Camel versies 4.14.6, 4.14.7, 4.18.1, 4.18.2, 4.19.0 en 4.20.0 om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- <https://camel.apache.org/security/CVE-2026-27172.html>
- <https://camel.apache.org/security/CVE-2026-33453.html>
- <https://camel.apache.org/security/CVE-2026-33454.html>
- <https://camel.apache.org/security/CVE-2026-40022.html>
- <https://camel.apache.org/security/CVE-2026-40048.html>
- <https://camel.apache.org/security/CVE-2026-40453.html>
- <https://camel.apache.org/security/CVE-2026-40473.html>
- <https://camel.apache.org/security/CVE-2026-40858.html>
- <https://camel.apache.org/security/CVE-2026-40860.html>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2026-27172	5.3 MEDIUM
➤ CVE-2026-33454	6.9 MEDIUM
➤ CVE-2026-40022	6.9 MEDIUM

> CVE-2026-40048	5.3 MEDIUM
> CVE-2026-40453	5.3 MEDIUM
> CVE-2026-40473	5.3 MEDIUM
> CVE-2026-40858	5.3 MEDIUM
> CVE-2026-40860	5.3 MEDIUM

CWE's

CWE	Beschrijving
> CWE-74	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')
> CWE-178	Improper Handling of Case Sensitivity
> CWE-287	Improper Authentication
> CWE-288	Authentication Bypass Using an Alternate Path or Channel
> CWE-502	Deserialization of Untrusted Data

Getroffen producten

Apache
Camel
Apache Software Foundation
Apache Camel
Apache Camel CoAP
Apache Camel Google PubSub

Apache Camel JMS
Apache Camel Mina
Apache Camel PQC
Apache Camel Platform HTTP Main

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.