



BULLETIN DE SECURITE

Titre	Vulnérabilités dans les produits Apache
Numéro de Référence	63612804/26
Date de Publication	28 Avril 2026
Risque	Important
Impact	Important

Systèmes affectés

- Apache MINA version 2.2.x antérieur à 2.2.5
- Apache MINA version 2.1.x antérieur à 2.1.10
- Apache MINA version 2.0.x antérieur à 2.0.27
- Apache Camel (Camel-Mail) version antérieure à 4.19.0
- Apache Camel (camel-coap) version 3.x. antérieur à 4.14.7
- Apache Camel (camel-coap) version 4.15.x antérieur à 4.18.2
- Apache Camel (camel-coap) version 4.19.x antérieur à 4.20.0
- Apache Camel (camel-jms) version 3.x. antérieur à 4.14.7
- Apache Camel (camel-jms) version 4.15.x antérieur à 4.18.2
- Apache Camel (camel-sjms) version 4.19.x antérieur à 4.20.0
- Apache Camel (camel-sjms) version 3.x. antérieur à 4.14.7
- Apache Camel (camel-sjms) version 4.15.x antérieur à 4.18.2
- Apache Camel (camel-google-pubsub)version 3.x. antérieur à 4.14.7
- Apache Camel (camel-google-pubsub)version 4.15.x antérieur à 4.18.2
- Apache Camel (camel-google-pubsub)version 4.19.x antérieur à 4.20.0
- Apache Camel (Camel-Infinispan)version 4.x antérieur à 4.14.7
- Apache Camel (Camel-Infinispan)version 4.15.x antérieur à 4.18.2
- Apache Camel (Camel-Infinispan)version 4.19.x antérieur à 4.20.0
- Apache Camel (Camel-pqc)version 4.18.x antérieur à 4.18.2
- Apache Camel (Camel-pqc)version 4.19.x antérieur à 4.20.0
- Apache Camel (Camel-camel-platform-http-main) version 4.14.x antérieur à 4.14.6

- Apache Camel (Camel-camel-platform-http-main) version 4.18.x antérieur à 4.18.2
- Apache Camel (Camel-leveldb)version 4.10.x antérieur à 4.10.9
- Apache Camel (Camel-leveldb)version 4.14.x antérieur à 4.14.5
- Apache Camel (Camel-leveldb)version 4.15.x antérieur à 4.18.0

Identificateurs externes

- CVE-2026-40453, CVE-2026-40860, CVE-2026-33453, CVE-2026-33454,
- CVE-2026-40858, CVE-2026-40048, CVE-2026-27172, CVE-2026-25747
- CVE-2026-41635 CVE-2026-41409

Bilan de la vulnérabilité

Plusieurs vulnérabilités ont été corrigées dans les produits Apache Camel et Apache Mina. L'exploitation de ces failles peut permettre à un attaquant distant d'exécuter du code arbitraire, d'injecter du contenu malveillant, de contourner les mécanismes de sécurité et d'accéder à des données sensibles.

Solution

Veillez se référer aux bulletins de sécurité Apache pour plus d'information.

Risque

- Exécution du code arbitraire à distance ;
- Accès aux informations confidentielles ;
- Injection de code arbitraire à distance ;

Annexe

Bulletins de sécurité Apache:

- <https://camel.apache.org/security/CVE-2026-40860.html>
- <https://camel.apache.org/security/CVE-2026-40858.html>
- <https://camel.apache.org/security/CVE-2026-40453.html>
- <https://camel.apache.org/security/CVE-2026-40048.html>
- <https://camel.apache.org/security/CVE-2026-33454.html>
- <https://camel.apache.org/security/CVE-2026-27172.html>
- <https://camel.apache.org/security/CVE-2026-25747.html>
- <https://lists.apache.org/thread/9ddvsq6c4l5bhwq8l14sob4f8qjvx5c9>
- <https://lists.apache.org/thread/1191w1mqsb3lwfd504fs045ylxntt2tm>