



BULLETIN DE SECURITE

Titre	Vulnérabilités dans Apache Tomcat
Numéro de Référence	61251902/26
Date de Publication	19 Février 2026
Risque	Important
Impact	Important

Systèmes affectés

- Apache Tomcat 11.0.x versions antérieures à 11.0.18 ;
- Apache Tomcat 10.1.x versions antérieures à 10.1.52 ;
- Apache Tomcat 9.0.x versions antérieures à 9.0.115 ;
- Apache Tomcat Native 1.3.x versions antérieures à 1.3.5 ;
- Apache Tomcat Native 2.0..x versions antérieures à 2.0.12;

Identificateurs externes

- CVE-2026-24734 ;

Bilan de la vulnérabilité

Apache Software Foundation a récemment publié une mise à jour de sécurité corrigéant une vulnérabilité affectant les versions susmentionnées du serveur Tomcat lors de l'utilisation d'un serveur OCSP (Online Certificate Status Protocol).

Le mécanisme ne traite pas correctement les vérifications d'authenticité et de validité des réponses OCSP. Cette faiblesse peut permettre le contournement de la vérification de révocation des certificats TLS, exposant les applications à l'acceptation de certificats potentiellement révoqués. L'exploitation de cette faille pourrait permettre à un attaquant de contourner la politique de sécurité et exposer les serveurs vulnérables aux attaques de type Man-in-the-Middle.

Solution

Veuillez se référer au bulletin de sécurité Apache Software Foundation pour plus d'information.

Risque

- Contournement de la politique de sécurité ;
- Exposition aux attaques de type Man-in-the-Middle;

Annexe

Bulletin de sécurité Apache Software Foundation:

- <https://lists.apache.org/thread/292dlmx3fz1888v6v16221kpozq56gml>
- <https://tomcat.apache.org/security-11.html>
- <https://tomcat.apache.org/security-10.html>
- <https://tomcat.apache.org/security-9.html>