aDvens

Security for the greater good

Bulletin d’alerte

Vulnérabilité critique dans Apache Struts

2023-12-14 | **TLP:CLEAR** | CERT aDvens - CTI

Advens - 16 Quai de la Mégisserie - 75001 Paris

Sommaire

CVE-2023-50164

Le 04 décembre 2023, Apache a émis un bulletin de sécurité concernant une vulnérabilité découverte au sein d'*Apache Struts 2*, identifiée sous la référence CVE-2023-50164.

Un défaut de contrôle des données dans la classe *Strusts ActionSupport*, permet à un attaquant distant et non authentifié, de téléverser un fichier malveillant dans un dossier ciblé pour exécuter une charge utile.

Le CERT-FR alerte dans son bulletin du 13 décembre 2023 sur l'existence d'une preuve de concept en sources ouvertes et de la possible exploitation de la vulnérabilité.

Des tentatives d'exploitation de la faille ont été constatées par l'ANSSI.

Type de vulnérabilité

- **CWE-552** : Files or Directories Accessible to External Parties

Risque

- Exécution de code arbitraire

Criticité (score de base CVSS v3.1)

Vecteur d'attaque	Réseau	Portée	Inchangée
Complexité d'attaque	Faible	Impact sur la confidentialité	Élevé
Privilèges requis	Aucun	Impact sur l'intégrité	Élevé
Interaction de l'utilisateur	Aucune	Impact sur la disponibilité	Élevé

Produits impactés

Versions Struts :

- Struts versions 2.x antérieures à 2.5.33
- Struts versions 6.x antérieures à 6.3.0.2

Recommandations

- Mettre à jour Apache Struts vers les versions 2.5.33, 6.3.0.2 ou ultérieures.
- Des informations complémentaires sont disponibles dans le bulletin de l'éditeur.

Preuve de concept

Une preuve de concept est disponible en sources ouvertes.

Références

- https://cwiki.apache.org/confluence/display/WW/s2-066
- https://www.cert.ssi.gouv.fr/alerte/CERTFR-2023-ALE-013/
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-50164