DJ-CERT
Centre national de veille, d'alerte et de réponse aux attaques informatiques

Autorité Nationale de Cybersécurité

Djibouti le, 13-09-2026

BULLETIN ALERTES

Object	Vulnérabilité dans AWS Systems Manager Agent
Réference	1501
Date de Publication	2026-09-10
Sévérité	Critique

IMPACT :

- Contournement de restrictions réseau (falsification de requêtes côté serveur, SSRF)
- Divulgation d'identifiants IAM temporaires
- Élévation de privilèges hors de l'instance concernée

SYSTÉME AFFECTÉ :

AWS Systems Manager Agent (SSM Agent) versions antérieures à 3.3.4851.0, toutes plateformes

DÉSCRIPTION :

Une vulnérabilité de falsification de requêtes côté serveur (SSRF) a été corrigée dans la fonctionnalité de redirection de port vers des hôtes distants de l'agent AWS Systems Manager. En raison d'une validation insuffisante des représentations équivalentes d'adresses réseau, un utilisateur authentifié disposant de la permission de rediriger des ports peut contourner la liste de destinations interdites et atteindre des points de terminaison locaux au lien (link-local), obtenant potentiellement les identifiants IAM temporaires associés au profil d'instance de la machine gérée.

SOLUTION :

Mettre à jour AWS Systems Manager Agent vers la version corrigée suivante :

- 3.3.4851.0 ou une version ultérieure

DOCUMENTATION :

Bulletin de sécurité AWS :

- https://aws.amazon.com/security/security-bulletins/2026-107-aws/

CVE-2026-89049 :

- https://www.cve.org/CVERecord?id=CVE-2026-89049