



## BULLETIN DE SECURITE

<b>Titre</b>	Vulnérabilités critiques dans Apache Traffic Server (ATS)
<b>Numéro de Référence</b>	51002011/24
<b>Date de Publication</b>	20 Novembre 2024
<b>Risque</b>	Critique
<b>Impact</b>	Critique

### Systemes affectés

- Apache Traffic Server (ATS) 9.x version antérieure à 9.2.6
- Apache Traffic Server (ATS) 10.x version antérieure à 10.0.2

### Identificateurs externes

- CVE-2024-38479, CVE-2024-50305, CVE-2024-50306

### Bilan de la vulnérabilité

Apache Software Foundation a récemment publié une mise à jour de sécurité pour Apache Traffic Server (ATS), qui corrige plusieurs vulnérabilités, dont une critique ayant de graves conséquences pour les systèmes affectés. Ces failles exposent ATS à des attaques pouvant entraîner l'empoisonnement du cache, des perturbations par déni de service (DoS) et une escalade des privilèges, ce qui pourrait permettre aux attaquants de prendre le contrôle total des serveurs concernés.

### Solution

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

### Risque

- Déni de service
- Elévation de privilèges
- Prise de contrôle du système affecté

### Annexe

Bulletin de sécurité Apache Software Foundation:

- <https://lists.apache.org/thread/y15fh6c7kyqvzm0f9odw7c5jh4r4np0y>