

# Mise à niveau du moteur Snort bloquée pendant la mise à niveau FTD en raison de la détection de stratégie personnalisée

## Table des matières

---

### Problème

Lors d'une mise à niveau FTD de la version 7.2 vers la version 7.4.4 sur un HA FPR-4115 géré par FMC, la mise à niveau du moteur Snort vers Snort 3 est bloquée avec des messages d'erreur indiquant l'échec de la conversion des règles personnalisées Snort 2 ou l'utilisation de stratégies d'intrusion ou d'analyse réseau personnalisées. Le message d'erreur spécifique indique : "Impossible d'effectuer la mise à niveau vers Snort 3. Le périphérique utilise au moins une stratégie d'intrusion personnalisée ou une stratégie d'analyse réseau." Un message d'échec plus détaillé fait référence à l'incapacité de convertir les règles personnalisées de Snort 2 et pointe vers `/var/sf/htdocs/ips/snort.rej` pour plus de détails. La préoccupation est de savoir si cette erreur empêcherait la migration vers Snort 3 et la fonctionnalité d'inspection d'impact.

### Environnement

- Cisco Secure Firewall Firepower version 7.3
- Firepower Management Center (FMC) version 7.7.11
- Périphériques FTD en configuration haute disponibilité (HA)
- Matériel : FPR-4115
- Chemin de mise à niveau : DFT 7.2 à 7.4.4
- VDB à la dernière version avant la mise à niveau
- La section Règles locales sous Objets > Règles d'intrusion > Snort 2 All Rules est vide

### Résolution

Le message d'erreur bloquant la mise à niveau du moteur Snort est un comportement documenté lié à l'ID de bogue Cisco CSCwn46794 et ne représente pas un bloqueur fonctionnel lorsqu'il n'existe aucune règle Snort 2 personnalisée.

### Étapes de vérification

Étape 1 : vérifiez l'état des règles Snort 2 personnalisées

Accédez à l'interface FMC et recherchez des règles Snort 2 personnalisées :

## Étape 2 : Confirmez la version de VDB

Avant de procéder à la mise à niveau, assurez-vous que la base de données des failles (VDB) est à la dernière version.

## Étape 3 : vérifiez les détails des erreurs

Vérifiez les informations d'erreur détaillées dans le fichier référencé :

```
/var/sf/htdocs/ips/snort.rej
```

## Processus de mise à niveau

Lorsque la section « Règles locales » est confirmée comme vide (aucune règle personnalisée Snort 2 n'est présente), la mise à niveau peut continuer malgré le message d'erreur. L'erreur de blocage est un faux positif dans ce scénario et n'indique pas les règles personnalisées réelles qui doivent être converties.

## Étape 1 : Passez à la mise à niveau Snort 3

Poursuivez le processus de mise à niveau FTD vers la version 7.4.4, qui inclut la mise à niveau du moteur Snort 3.

## Étape 2 : Validation post-mise à niveau

Une fois la mise à niveau terminée, testez le flux de trafic pour confirmer le comportement attendu avec le moteur Snort 3.

## Étape 3 : Surveillez les performances du système

Vérifiez que la fonctionnalité d'inspection fonctionne comme prévu avec le nouveau moteur Snort 3.

## Motif

Le message de blocage de la mise à niveau est un comportement documenté associé à l>ID de bogue Cisco CSCwn46794. Ce bogue entraîne l'affichage d'un message d'erreur sur les stratégies d'intrusion personnalisées ou les stratégies d'analyse réseau même lorsqu'il n'existe aucune règle Snort 2 personnalisée réelle nécessitant une conversion. Le message d'erreur apparaît comme un faux positif lorsque la section Règles locales est vide, mais la validation de pré-mise à niveau du système identifie de manière incorrecte la présence de stratégies personnalisées.

## Autres informations utiles

- [ID de bogue Cisco CSCwn46794](#)
- [ID de bogue Cisco CSCwk07199](#)
- [Assistance technique de Cisco et téléchargements](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.