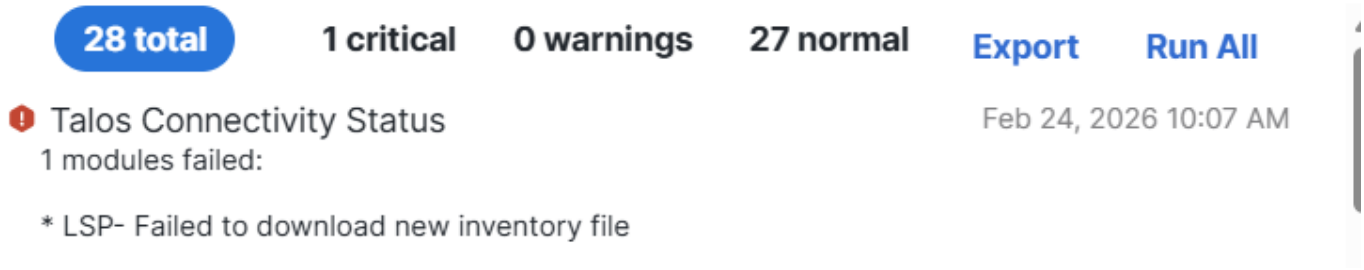
Mises à jour automatiques FMC LSP " ; Échec du téléchargement du nouvel inventaire" ;

Problème

Les mises à jour LSP (Lightweight Security Package) automatiques échouent sur Cisco FMC. Les mises à jour LSP ne s'installent plus automatiquement, tandis que l'installation LSP manuelle continue de fonctionner correctement. Les mises à jour VDB et les mises à jour de règle Snort continuent de fonctionner normalement via des processus automatiques.

Exemple d'alerte



image_en_ligne_0.png

Environnement

- Cisco Secure Firewall Firepower Management Center 7.6.x On-Prem (applicable à tous les modèles FMC et versions 7.6+)

Résolution

Pour résoudre l’échec de la mise à jour automatique du LSP, vérifiez que la connectivité réseau requise est correctement configurée sur les pare-feu ou les périphériques réseau en amont

susceptibles de bloquer le processus de mise à jour.

1 : Vérifier l'état actuel de la version LSP

Vérifiez la version actuelle du LSP installée sur le périphérique Firepower Threat Defense :

```
show version
```

Exemple de sortie montrant la version actuelle du LSP :

```
--------------[ périphérique ]--------------

Modèle : Cisco Secure Firewall 3140 Threat Defense (80) Version 7.6.2.1 (Build 3)

UUID : 5fb22700-68c8-11ee-b5a0-d2e6638aec56

Version de LSP : lsp-rel-20260121-2008

Version VDB : 421

--------------------------------------------------
```

2 : Vérifier les besoins en connectivité réseau

Assurez-vous que l'accès sortant sur le port 80 est autorisé sur tout pare-feu en amont ou périphérique de sécurité réseau pour ces destinations :

- updates-dyn-talos.sco.cisco.com - Requis pour les mises à jour LSP
- updates.ironport.com - Requis pour les mises à jour du contenu de sécurité

Ces destinations sont essentielles au bon fonctionnement du processus de mise à jour automatique. Tout blocage de ces connexions empêche les mises à jour LSP automatiques tout en permettant aux mises à jour manuelles de fonctionner.

Exemple de test de connexion de FMC avec erreur

```
root@fmc:/Volume/home/user# curl -v -k http://updates.ironport.com
```

```
<h1>Page Web bloquée</h1>

 <p>La page Web que vous essayez de visiter a été bloquée conformément à la stratégie de la société. Contactez votre administrateur système si vous pensez qu'il s'agit d'une erreur.</p>
```

Exemples de journaux d'erreurs provenant de /var/log/sf/talos_agent.log

```
sf/talos_agent.log:TalosAgent:ERROR:
```
updater.go:talosagent.cisco.com/pkg/updater.UpdateService:475 2026/02/13 04:11:05 Failed to downloac
```
error: code = Internal desc = http error 503 Service Unavailable while downloading file
204cf9af41f70cb30cfd3a7d41ab2f7366219cbfa805b4ec743bb957f373b87630d8e4027491747102d060ed5e238ab
```

sf/talos_agent.log:TalosAgent:ERROR:
updater.go:talosagent.cisco.com/pkg/updater.UpdateService:475 2026/02/24 19:18:08 Failed to downloac
failed: connection error: Connection reset by peer (erreur OS 104)

3 : vérification de la configuration de mise à jour

Vérifiez que les mises à jour automatiques sont correctement configurées dans le Centre de gestion du pare-feu pour les mises à jour LSP. Le fait que les mises à jour de règles VDB et Snort continuent à fonctionner automatiquement suggère que le mécanisme de mise à jour de base est fonctionnel, mais que la connectivité spécifique au LSP peut être bloquée.

4 : Tester la connectivité

Après avoir vérifié que les destinations requises sont accessibles via les périphériques de sécurité en amont, surveillez le processus de mise à jour automatique pour vérifier que les mises à jour LSP reprennent un fonctionnement normal.

Exemple de sortie de travail

```
root@echo-ngfw-fmcv3:/Volume/home/admin# curl -v -k http://updates.ironport.com
```

```
* Essai en cours 208.90.58.25:80...
```

```
* Connecté au port 80 de updates.ironport.com (208.90.58.25) (#0)
```

```
> GET / HTTP/1.1

> Hôte : updates.ironport.com

> User-Agent : curl/7.79.1

> Accepter : */*

>

* Marquer le bundle comme ne prenant pas en charge la multiutilisation

< HTTP/1.1 200 OK

< Serveur : nginx/1.20.1

< Date : Lun, 16 Mar 2026 20:22:35 GMT

< Content-Type : text/html

< Longueur du contenu : 689

< Dernière modification : mer, 06 sept. 2006 17:26:12 GMT

< Connexion : keep-alive

< ETag : "44ff04b4-2b1"

< Expire le : mar., 17 mars 2026 20:22:35 GMT

< Cache-Control : max-age=86400

< Plages d'acceptation : octets

<

<HTML>
```

```
  <!- $En-tête : /usr/local/cvsroot/godspeed/upgrade_server/http/html/root.html,v 1.1 2004/06/25
22:43:59 Brie Exp $ ->

  <EN-TÊTE>

  </HEAD>

  <CORPS>

    <IMG SRC="http://ironport.com/media/logo.gif">

    <P>

      Il s'agit du serveur de mise à jour IronPort. Si vous essayez de télécharger de nouveaux

de surveillance du trafic, de merlin ou de paquets WBRS, vous avez atteint cette page par
erreur.

  Reportez-vous aux notes de version de Update Manager pour obtenir des instructions de
téléchargement

le nouveau logiciel.

    </P>

    <P>

      Pour toute question, n'hésitez pas à contacter le service client IronPort

      au (877)641-4766 ou à l'adresse <A
HREF="mailto:support@ironport.com">support@ironport.com</A>.

    </P>

  </BODY>

</HTML>
```

```
* La connexion #0 à l'hôte updates.ironport.com est restée intacte
```

Assurez-vous que le périphérique respecte les exigences requises pour la connectivité des ports et des domaines pour les autres types de mise à jour et de téléchargement, comme indiqué dans la documentation publique de Cisco :

- Guide d'administration de Cisco Secure Firewall Management Center, 7.6 : Sécurité, accès à Internet et ports de communication

Motif

L'échec de la mise à jour automatique du LSP est causé par une connectivité réseau bloquée aux serveurs de mise à jour requis. Plus précisément, l'accès sortant via le port 80 aux mises à jour-dyn-talos.sco.cisco.com et updates.ironport.com est restreint par des règles de pare-feu en amont ou des stratégies de sécurité réseau. Cela empêche le FMC de télécharger et d'installer automatiquement les mises à jour du LSP, tandis que les mises à jour manuelles peuvent toujours être effectuées car elles peuvent utiliser différentes méthodes de téléchargement ou du contenu mis en cache.

Toutefois, le problème peut également être affecté par la capacité du FMC à télécharger des fichiers volumineux à partir du site cloud Cisco. La limitation de la bande passante du FMC, associée à d'autres mises à jour logicielles multiples (par exemple, SRU et VDB) dans le même délai, peut entraîner une concurrence pour la bande passante, ce qui entraîne des échecs de téléchargement. Dans ce cas, séparez les durées de téléchargement du logiciel pour leur permettre de disposer de suffisamment de bande passante pour les téléchargements ou pour résoudre les problèmes de bande passante en amont.

Autres informations utiles

- Assistance technique de Cisco et téléchargements
- Guide d'administration de Cisco Secure Firewall Management Center, 7.6 : Sécurité, accès à Internet et ports de communication

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.