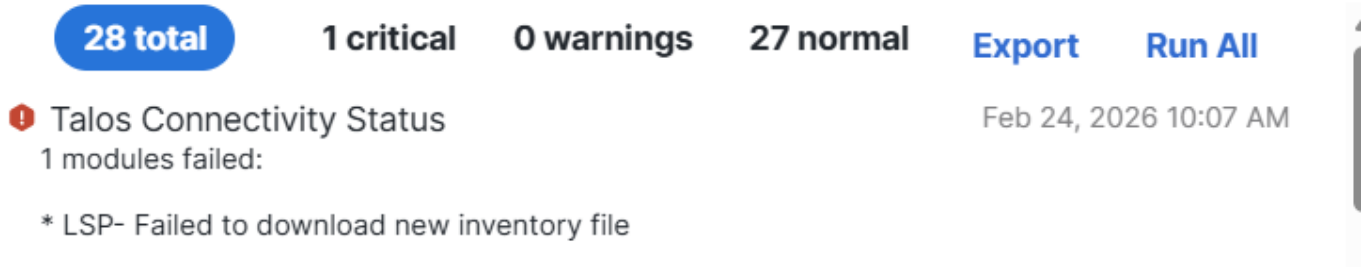
FMC Automatic LSP Updates "Failed to download new Inventory"

Problema

Las actualizaciones automáticas del paquete ligero de seguridad (LSP) están fallando en Cisco FMC. Las actualizaciones de LSP ya no se instalan automáticamente, mientras que la instalación manual de LSP sigue funcionando correctamente. Las actualizaciones de VDB y las actualizaciones de reglas de Snort siguen funcionando normalmente mediante procesos automáticos.

Ejemplo de alerta



inline_image_0.png

Entorno

- Cisco Secure Firewall Firepower Management Center 7.6.x en las instalaciones (aplicable a todos los modelos FMC y versiones 7.6 o posteriores)

Resolución

Para resolver la falla de actualización automática de LSP, verifique que la conectividad de red

requerida esté configurada correctamente en cualquier firewall ascendente o dispositivo de red que pueda estar bloqueando el proceso de actualización.

1: Verificar el estado actual de la versión de LSP

Compruebe la versión actual de LSP instalada en el dispositivo Firepower Threat Defence:

```
show version
```

Ejemplo de salida que muestra la versión actual de LSP:

```
--------------[ dispositivo ]--------------

Modelo: Cisco Secure Firewall 3140 Threat Defense (80) Versión 7.6.2.1 (Compilación 3)

UUID: 5fb22700-68c8-11ee-b5a0-d2e638aec56

Versión de LSP: lsp-rel-20260121-2008

Versión de VDB: 421

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

2: Verificar los requisitos de conectividad de red

Asegúrese de que se permite el acceso saliente a través del puerto 80 en cualquier firewall ascendente o dispositivo de seguridad de red para estos destinos:

- updates-dyn-talos.sco.cisco.com: necesario para las actualizaciones de LSP
- updates.ironport.com: necesario para las actualizaciones de contenido de seguridad

Estos destinos son esenciales para que el proceso de actualización automática funcione correctamente. Cualquier bloqueo de estas conexiones evita las actualizaciones LSP automáticas y permite que funcionen las actualizaciones manuales.

Ejemplo de prueba de conexión de FMC con error

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

<h1>Página web bloqueada</h1>

 <p>La página web que intenta visitar se ha bloqueado de acuerdo con la política de la empresa.
Póngase en contacto con el administrador del sistema si cree que se trata de un error.</p>
```

Registros de error de ejemplo 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 Servicio no disponible al descargar el archivo
204cf9af41f70cb30cfd3a7d41ab2f7366219cbfa805b4ec7443bb957f373b87630d8e4027491747102d060ed5e238ab
```

sf/talos_agent.log:TalosAgent:ERROR:
updater.go:talosagent.cisco.com/pkg/updater.UpdateService:475 2026/02/24 19:18:08 Failed to downloac
falló: error de conexión: conexión restablecida por el par (error de sistema operativo 104)

3: Verificar configuración de actualización

Confirme que las actualizaciones automáticas estén configuradas correctamente en el Centro de administración de firewall para las actualizaciones de LSP. El hecho de que las actualizaciones de VDB y de reglas de Snort continúen funcionando automáticamente sugiere que el mecanismo de actualización básico funciona, pero que la conectividad específica de LSP se puede bloquear.

4: Pruebe la conectividad

Después de confirmar que se puede acceder a los destinos requeridos a través de cualquier dispositivo de seguridad ascendente, supervise el proceso de actualización automática para verificar que las actualizaciones de LSP reanudan el funcionamiento normal.

Ejemplo de resultado de trabajo

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

* Intentando 208.90.58.25:80...

* Conectado a updates.ironport.com (208.90.58.25) puerto 80 (#0)
```

```
> GET / HTTP/1.1

> Host: updates.ironport.com

> User-Agent: curl/7.79.1

> Aceptar: */*

>

* Marcar el paquete como no compatible con multiusos

< HTTP/1.1 200 OK

< Servidor: nginx/1.20.1

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

< Content-Type: text/html

< Content-Length: 689

< Última modificación: miércoles 6 de septiembre de 2006 17:26:12 GMT

< Conexión: keepalive

< ETag: "44ff04b4-2b1"

< Expira: martes, 17 de marzo de 2026 20:22:35 GMT

< Cache-Control: max-age=86400

< Accept-Ranges: bytes

<

<HTML>
```

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

<HEAD>

</HEAD>

<BODY>

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

<P>

Este es el servidor de actualización de IronPort. Si está intentando descargar nuevo monitor de tráfico, merlin o paquetes WBRS, ha llegado a esta página por error.

Consulte las notas de la versión de Update Manager para obtener instrucciones para la descarga el nuevo software.

</P>

<P>

Si tiene alguna pregunta, no dude en ponerse en contacto con Atención al cliente de IronPort

al (877)641-4766 o <A HREF="mailto:support@ironport.com">support@ironport.com</A>.

</P>

</BODY>

</HTML>

* Se ha dejado intacta la conexión #0 al host updates.ironport.com

Asegúrese de que el dispositivo cumpla con los requisitos necesarios para la conectividad de puerto y dominio para otros diversos tipos de actualización y descarga, como se indica en la documentación pública de Cisco:

- Guía de administración de Cisco Secure Firewall Management Center, 7.6: seguridad, acceso a Internet y puertos de comunicación

Causa

El fallo de actualización automática de LSP se debe a un bloqueo de la conectividad de red con los servidores de actualización necesarios. En concreto, el acceso saliente a través del puerto 80 a updates-dyn-talos.sco.cisco.com y updates.ironport.com está restringido por las reglas de firewall ascendentes o las políticas de seguridad de la red. Esto impide que el FMC descargue e instale automáticamente actualizaciones de LSP, mientras que las actualizaciones manuales se pueden seguir realizando porque pueden utilizar diferentes métodos de descarga o contenido almacenado en caché.

Sin embargo, el problema también puede verse afectado por la capacidad del FMC para descargar archivos de gran tamaño desde el sitio en la nube de Cisco. La limitación del ancho de banda del FMC, junto con otras actualizaciones de software múltiples (es decir, SRU y VDB) dentro del mismo período de tiempo, puede generar competencia por el ancho de banda, lo que puede dar lugar a fallos de descarga. En estos casos, separe los tiempos de descarga del software para permitirles un ancho de banda suficiente para las descargas o resuelva cualquier problema de ancho de banda ascendente.

Contenido relacionado

- Soporte técnico y descargas de Cisco
- Guía de administración de Cisco Secure Firewall Management Center, 7.6: seguridad, acceso a Internet y puertos de comunicación

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).