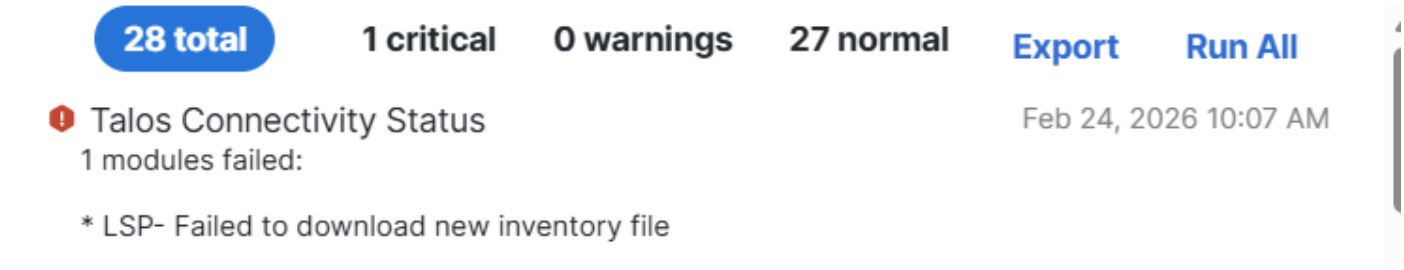
"Aggiornamenti LSP automatici FMC: impossibile scaricare nuovo inventario"

Problema

Impossibile eseguire gli aggiornamenti LSP (Lightweight Security Package) automatici in Cisco FMC. Gli aggiornamenti LSP non vengono più installati automaticamente, mentre l'installazione manuale LSP continua a funzionare correttamente. Gli aggiornamenti VDB e le regole Snort funzionano ancora normalmente tramite processi automatici.

Avviso di esempio



inline_image_0.png

Ambiente

- Cisco Secure Firewall Firepower Management Center 7.6.x in locale (applicabile a tutti i modelli e le versioni 7.6+ di FMC)

Risoluzione

Per risolvere l'errore di aggiornamento LSP automatico, verificare che la connettività di rete richiesta sia configurata correttamente in tutti i firewall upstream o i dispositivi di rete che

potrebbero bloccare il processo di aggiornamento.

1: Verificare lo stato della versione corrente dell'LSP

Controllare la versione LSP corrente installata sul dispositivo Firepower Threat Defense:

```
show version
```

Output di esempio che mostra la versione LSP corrente:

```
-[ dispositivo ]-

Modello: Cisco Secure Firewall 3140 Threat Defense (80) versione 7.6.2.1 (Build 3)

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

Versione LSP : lsp-rel-20260121-2008

Versione VDB: 421

-
```

2: Verificare i requisiti di connettività di rete

Verificare che l'accesso in uscita tramite la porta 80 sia consentito su qualsiasi firewall a monte o dispositivo di sicurezza di rete per le seguenti destinazioni:

- updates-dyn-talos.sco.cisco.com - Richiesto per gli aggiornamenti LSP
- updates.ironport.com - Necessario per gli aggiornamenti del contenuto di protezione

Queste destinazioni sono essenziali per il corretto funzionamento del processo di aggiornamento automatico. Eventuali blocchi di queste connessioni impediscono gli aggiornamenti automatici dei provider di servizi di traduzione consentendo al tempo stesso il funzionamento degli aggiornamenti manuali.

Esempio di test di connessione da FMC con errore

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

<h1>Pagina Web bloccata</h1>

 <p>La pagina Web che si sta tentando di visitare è stata bloccata in conformità ai criteri aziendali. Se si ritiene che si tratti di un errore, contattare l'amministratore di sistema.</p>
```

Esempi di log degli errori da /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
204cf9af41f70cb30cfd3a7d41ab2f736219cbfa805b4ec7443bb957f373b87630d8e4027491747102d060ed5e238ab
```

sf/talos_agent.log:TalosAgent:ERROR:
updater.go:talosagent.cisco.com/pkg/updater.UpdateService:475 2026/02/24 19:18:08 Failed to downloac
non riuscito: errore di connessione: connessione reimpostata dal peer (errore sistema operativo
104)

3: Verifica della configurazione dell'aggiornamento

Verificare che gli aggiornamenti automatici siano configurati correttamente in Centro gestione firewall per gli aggiornamenti LSP. Il fatto che gli aggiornamenti delle regole VDB e Snort continuino a funzionare indica che il meccanismo di aggiornamento di base è funzionante, ma la connettività specifica di LSP può essere bloccata.

4: Test della connettività

Dopo aver verificato che le destinazioni richieste siano accessibili tramite dispositivi di sicurezza a monte, monitorare il processo di aggiornamento automatico per verificare che gli aggiornamenti LSP riprendano il normale funzionamento.

Esempio di output di lavoro

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

* Prova 208.90.58.25:80...
```

```
* Connesso alla porta 80 (#0) di updates.ironport.com (208.90.58.25)

> GET/HTTP/1.1

> Host: updates.ironport.com

> Agente utente: curl/7.79.1

> Accettazione: */*

>

* Contrassegnare il bundle come non compatibile multiuso

< HTTP/1.1 200 OK

< Server: Inginx/1.20.1

< Data: lun, 16 mar 2026 20:22:35 GMT

< Content-Type: testo/html

< Lunghezza contenuto: 689

< Ultima modifica: Mer, 06 set 2006 17:26:12 GMT

< Connessione: keep-alive

< ETag: "44ff04b4-2b1"

< Scade: mar, 17 mar 2026 20:22:35 GMT

< Cache-Control: max-age=86400

< Accept-Ranges: byte

<
```

```
<HTML

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

  <HEAD>

  </HEAD>

  <CORPO>

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

    <P>

      Server di aggiornamento IronPort. Se si sta tentando di scaricare un nuovo

i pacchetti traffic monitor, merlin o WBRS, hai raggiunto questa pagina per errore.

  Consultare le note di rilascio di Update Manager per istruzioni sul download

il nuovo software.

    </P>

    <P>

      In caso di domande, contatta l'Assistenza clienti IronPort

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

    </P>

  </BODY>

</HTML>
```

```
* Connessione n. 0 per l'host updates.ironport.com rimasta intatta
```

Verificare che il dispositivo rispetti i requisiti necessari per la connettività della porta e del dominio per altri tipi di aggiornamento e download, come indicato nella documentazione pubblica di Cisco:

- Cisco Secure Firewall Management Center Administration Guide, 7.6: Security, Internet Access, and Communication Ports

Causa

L'errore di aggiornamento LSP automatico è causato dal blocco della connettività di rete ai server di aggiornamento richiesti. In particolare, l'accesso in uscita dalla porta 80 agli aggiornamenti-dyn-talos.sco.cisco.com e updates.ironport.com è soggetto a restrizioni da regole firewall upstream o criteri di sicurezza di rete. Ciò impedisce al FMC di scaricare e installare automaticamente gli aggiornamenti LSP, mentre è ancora possibile eseguire gli aggiornamenti manuali perché possono utilizzare metodi di download o contenuto memorizzato nella cache diversi.

Tuttavia, il problema può anche essere influenzato dalla capacità del FMC di scaricare file di grandi dimensioni dal sito cloud Cisco. Limitare la larghezza di banda del FMC, insieme ad altri aggiornamenti software multipli (ad esempio SRU e VDB) entro lo stesso periodo di tempo può stabilire una competizione per la larghezza di banda che porta a errori di download. In questi casi, separare i tempi di download del software per consentire loro una larghezza di banda sufficiente per i download o risolvere eventuali problemi di larghezza di banda upstream.

Contenuto correlato

- Supporto tecnico Cisco e download
- Cisco Secure Firewall Management Center Administration Guide, 7.6: Security, Internet Access, and Communication Ports

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).