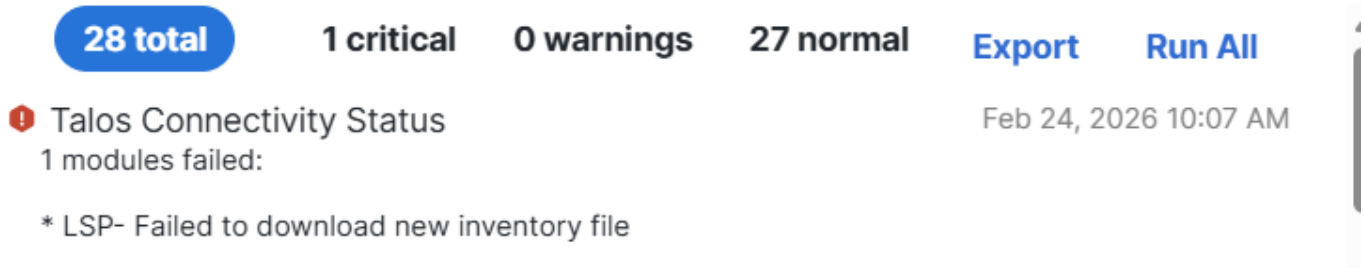
Atualizações automáticas de LSP do FMC "Falha no download do novo inventário"

Problema

As atualizações automáticas do Lightweight Security Package (LSP) estão falhando no Cisco FMC. As atualizações do LSP não são mais instaladas automaticamente, enquanto a instalação manual do LSP continua a funcionar corretamente. As atualizações do VDB e das regras de Snort ainda estão funcionando normalmente por meio de processos automáticos.

Exemplo de alerta



inline_image_0.png

Ambiente

- Cisco Secure Firewall Firepower Management Center 7.6.x On-Prem (aplicável a todos os modelos FMC e versões 7.6+)

Resolução

Para resolver a falha de atualização automática de LSP, verifique se a conectividade de rede necessária está configurada corretamente em todos os firewalls ou dispositivos de rede upstream

que possam estar bloqueando o processo de atualização.

1: Verificar o status da versão atual do LSP

Verifique a versão atual do LSP instalada no dispositivo Firepower Threat Defense:

```
show version
```

Exemplo de saída mostrando a versão atual do LSP:

```
--------------[ device ]--------------

Modelo: Cisco Secure Firewall 3140 Threat Defense (80) Versão 7.6.2.1 (Build 3)

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

Versão LSP : lsp-rel-20260121-2008

Versão do VDB: 421

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

2: Verificar os requisitos de conectividade de rede

Verifique se o acesso de saída pela porta 80 é permitido em qualquer firewall de upstream ou dispositivo de segurança de rede para estes destinos:

- updates-dyn-talos.sco.cisco.com - Necessário para atualizações LSP
- updates.ironport.com - Necessário para atualizações de conteúdo de segurança

Esses destinos são essenciais para que o processo de atualização automática funcione corretamente. Qualquer bloqueio dessas conexões impede atualizações LSP automáticas, permitindo ainda que as atualizações manuais funcionem.

Exemplo de teste de conexão do FMC com erro

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

<h1>Página da Web Bloqueada</h1>

 <p>A página da Web que você está tentando visitar foi bloqueada de acordo com a política da empresa. Entre em contato com o administrador do sistema se achar que isso é um erro.</p>
```

Exemplo de logs de erro 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
erro: código = Internal desc = http error 503 Serviço Indisponível durante o download do arquivo
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
falhou: erro de conexão: Conexão redefinida pelo par (erro de sistema operacional 104)
```

3: Verificar configuração de atualização

Confirme se as atualizações automáticas estão configuradas corretamente no Centro de Gerenciamento de Firewall para atualizações de LSP. O fato de que as atualizações de regras VDB e Snort continuam a funcionar automaticamente sugere que o mecanismo de atualização básico está funcionando, mas a conectividade específica de LSP pode ser bloqueada.

4: Testar a conectividade

Depois de confirmar que os destinos necessários estão acessíveis por meio de qualquer dispositivo de segurança upstream, monitore o processo de atualização automática para verificar se as atualizações de LSP reiniciam a operação normal.

Exemplo de saída de trabalho

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

* Tentando 208.90.58.25:80...

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

```
> GET / HTTP/1.1

> Host:  updates.ironport.com

> User-Agent: curl/7.79.1

> Aceitar: */*

>

* Marcar o pacote como não compatível com vários usuários

< HTTP/1.1 200 OK

< Servidor: nginx/1.20.1

< Data: Seg, 16 de março de 2026 20:22:35 GMT

< Tipo de conteúdo: text/html

< Comprimento do conteúdo: 689

< Última modificação: Qua, 06 set 2006 17:26:12 GMT

< Conexão: keep-alive

< ETag: "44ff04b4-2b1"

< Vence em: Ter, 17 de março de 2026 20:22:35 GMT

< Cache-Control: max-age=86400

< Intervalos aceitos: 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>

<CORPO>

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

<P>

Este é o Servidor de Atualização IronPort. Se você estiver tentando baixar novos pacotes de monitor de tráfego, merlin ou WBRS, você chegou a esta página por engano.

Consulte as Notas de versão do Update Manager para obter instruções de download o novo software.

</P>

<P>

Em caso de dúvidas, entre em contato com o Atendimento ao cliente IronPort

no telefone (877)641-4766 ou <A HREF="mailto:support@ironport.com">support@ironport.com</A>.

</P>

</CORPO>

</HTML>

* #0 de conexão para atualizações de host.ironport.com deixado intacto

Assegure-se de que o dispositivo cumpra os requisitos necessários para conectividade de porta e domínio para vários outros tipos de atualização e download, conforme declarado na documentação pública da Cisco:

- Guia de Administração do Cisco Secure Firewall Management Center, 7.6: Segurança, Acesso à Internet e Portas de Comunicação

Causa

A falha de atualização automática de LSP é causada pela conectividade de rede bloqueada com os servidores de atualização necessários. Especificamente, o acesso de saída pela porta 80 para updates-dyn-talos.cisco.com e updates.ironport.com está sendo restringido pelas regras de firewall de upstream ou pelas políticas de segurança de rede. Isso impede que o FMC baixe e instale automaticamente atualizações de LSP, enquanto atualizações manuais ainda podem ser executadas porque podem usar métodos de download diferentes ou conteúdo armazenado em cache.

No entanto, o problema também pode ser afetado pela capacidade do FMC de baixar arquivos grandes do site de nuvem da Cisco. A limitação da largura de banda do FMC, juntamente com outras atualizações de software (ou seja, SRU e VDB) dentro do mesmo período de tempo, pode configurar a competição por largura de banda levando a falhas de download. Nesses casos, separe os tempos de download de software para permitir que eles tenham largura de banda suficiente para downloads ou resolva quaisquer problemas de largura de banda upstream.

Conteúdo relacionado

- Suporte técnico e downloads da Cisco
- Guia de Administração do Cisco Secure Firewall Management Center, 7.6: Segurança, Acesso à Internet e Portas de Comunicação

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.