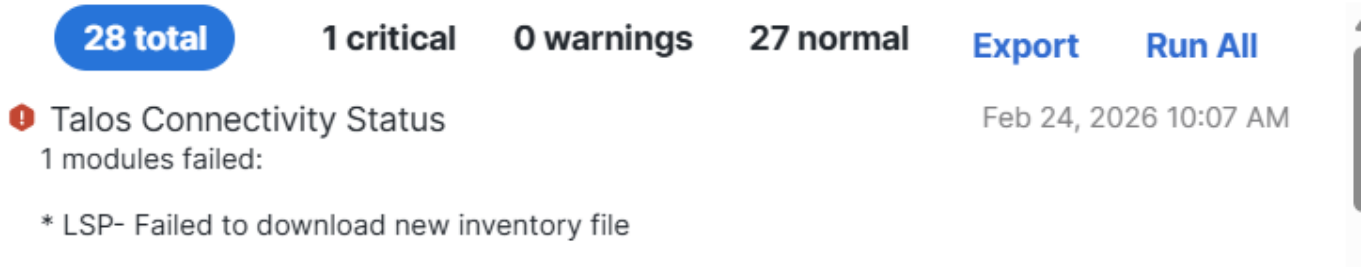
Automatische LSP-Aktualisierungen für FMC "Neuer Bestand konnte nicht heruntergeladen werden"

Problem

Die automatischen LSP-Updates (Lightweight Security Package) funktionieren auf Cisco FMC nicht. LSP-Updates werden nicht mehr automatisch installiert, während die manuelle LSP-Installation weiterhin ordnungsgemäß funktioniert. VDB-Updates und Snort-Regel-Updates funktionieren weiterhin normal über automatische Prozesse.

Beispielbenachrichtigung



inline_image_0,png

Umwelt

- Cisco Secure Firewall FirePOWER Management Center 7.6.x (für alle FMC-Modelle und -Versionen 7.6+)

Auflösung

Überprüfen Sie zur Behebung des automatischen LSP-Update-Fehlers, ob die erforderliche Netzwerkverbindung auf den Upstream-Firewalls oder Netzwerkgeräten, die den Update-Prozess blockieren könnten, ordnungsgemäß konfiguriert ist.

1: Überprüfen des aktuellen LSP-Versionsstatus

Überprüfen Sie die aktuelle LSP-Version, die auf dem Firepower Threat Defense-Gerät installiert ist:

```
show version
```

Beispielausgabe mit der aktuellen LSP-Version:

```
--------------[ Gerät ]--------------

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

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

LSP-Version: lsp-rel-20260121-2008

VDB-Version: 421

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

2: Überprüfen der Anforderungen an die Netzwerkverbindungen

Stellen Sie sicher, dass der ausgehende Zugriff über Port 80 auf jeder Upstream-Firewall oder jedem Netzwerksicherheitsgerät für diese Ziele zugelassen wird:

- updates-dyn-talos.sco.cisco.com - Erforderlich für LSP-Updates
- updates.ironport.com - Erforderlich für Aktualisierungen von Sicherheitsinhalten

Diese Ziele sind wichtig, damit der automatische Aktualisierungsprozess ordnungsgemäß funktioniert. Jede Blockierung dieser Verbindungen verhindert automatische LSP-Aktualisierungen, während gleichzeitig manuelle Aktualisierungen möglich sind.

Beispielverbindungstest von FMC mit Fehler

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

```
<h1>Webseite blockiert</h1>
```

```
 <p>Die Webseite, die Sie aufrufen möchten, wurde gemäß den Unternehmensrichtlinien gesperrt.
Wenden Sie sich an Ihren Systemadministrator, wenn Sie glauben, dass dies ein Fehler ist.</p>
```

Beispiele für Fehlerprotokolle von /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 Nicht verfügbar beim Herunterladen der
Datei
204cf9af41f70cb30cfd3a7d41ab2f7366219cbfa805b4ec7443bb957f373b87630d8e4027491747102d060ed5ab
e238ab
```

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 (os error 104)

3: Überprüfen der Update-Konfiguration

Bestätigen Sie, dass automatische Updates im Firewall Management Center für LSP-Updates ordnungsgemäß konfiguriert sind. Die Tatsache, dass Updates von VDB- und Snort-Regeln weiterhin automatisch funktionieren, deutet darauf hin, dass der grundlegende Aktualisierungsmechanismus funktioniert, jedoch können LSP-spezifische Verbindungen blockiert werden.

4: Testen der Verbindung

Nachdem sichergestellt wurde, dass die erforderlichen Ziele über alle Upstream-Sicherheitsgeräte erreichbar sind, überwachen Sie den automatischen Update-Prozess, um sicherzustellen, dass die LSP-Updates den normalen Betrieb wieder aufnehmen.

Beispiel einer Arbeitsleistung

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

* 208.90.58.25:80 wird versucht...

* Verbunden mit updates.ironport.com (208.90.58.25) Port 80 (#0)

> GET/HTTP/1.1

> Host: updates.ironport.com

> User-Agent: curl/7.79.1

> Akzeptieren: */*

>

* Markieren Sie das Paket als nicht unterstützend für mehrere Benutzer.

< HTTP/1.1 200 OK

< Server: nginx/1.20.1

< Datum: Mo, 16 Mär 2026 20:22:35 GMT

< Inhaltstyp: text/html

< Inhaltslänge: 689

< Zuletzt geändert: Mittwoch, 06. September 2006, 17:26:12 Uhr GMT

< Verbindung: keep-alive

< ETag: 44ff04b4-2b1"

< Gültig bis: Dienstag, 17. März 2026, 20:22:35 Uhr GMT

< Cache-Control: max-age=86400
```

< Akzeptieren-Bereiche: Bytes

<

<HTML>

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

  <ÜBERSCHRIFT>

  </HEAD>

  <TEXT>

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

    <P>

      Dies ist der IronPort-Aktualisierungsserver. Wenn Sie versuchen, neue Traffic Monitor-, Merlin- oder WBRS-Pakete haben Sie diese Seite irrtümlicherweise erreicht.

  Anweisungen zum Herunterladen finden Sie in den Update Manager-Versionshinweisen.

die neue Software.

    </P>

    <P>

      Bei Fragen können Sie sich jederzeit an den IronPort Kundenservice wenden.

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

    </P>

```
  </BODY>

</HTML>

* Verbindung #0 zu Host updates.ironport.com bleibt intakt
```

Stellen Sie sicher, dass das Gerät die erforderlichen Anforderungen für die Port- und Domänenkonnektivität für andere Update- und Download-Typen erfüllt, wie in der öffentlichen Dokumentation von Cisco beschrieben:

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

Ursache

Der Fehler bei der automatischen LSP-Aktualisierung wird durch die blockierte Netzwerkverbindung zu den erforderlichen Aktualisierungsservern verursacht. Insbesondere wird der ausgehende Zugriff über Port 80 auf updates-dyn-talos.sco.cisco.com und updates.ironport.com durch Upstream-Firewall-Regeln oder Netzwerksicherheitsrichtlinien eingeschränkt. Dadurch wird verhindert, dass das FMC automatisch LSP-Updates herunterlädt und installiert, während weiterhin manuelle Updates durchgeführt werden können, da sie unterschiedliche Downloadmethoden oder zwischengespeicherten Inhalt verwenden können.

Das Problem kann jedoch auch dadurch beeinträchtigt werden, dass das FMC große Dateien von der Cisco Cloud-Website herunterladen kann. Eine Drosselung der FMC-Bandbreite in Verbindung mit mehreren Software-Updates (d. h. SRU und VDB) innerhalb desselben Zeitrahmens kann zu einem Bandbreitenwettbewerb führen, der zu Download-Fehlern führt. In solchen Fällen müssen Sie die Software-Download-Zeiten so lange trennen, dass genügend Bandbreite für Downloads verfügbar ist, oder mögliche Upstream-Bandbreitenprobleme lösen.

Verwandte Inhalte

- Technischer Support und Downloads von Cisco
- Cisco Secure Firewall Management Center Administration Guide, 7.6: Security, Internet Access und Communication Ports

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.