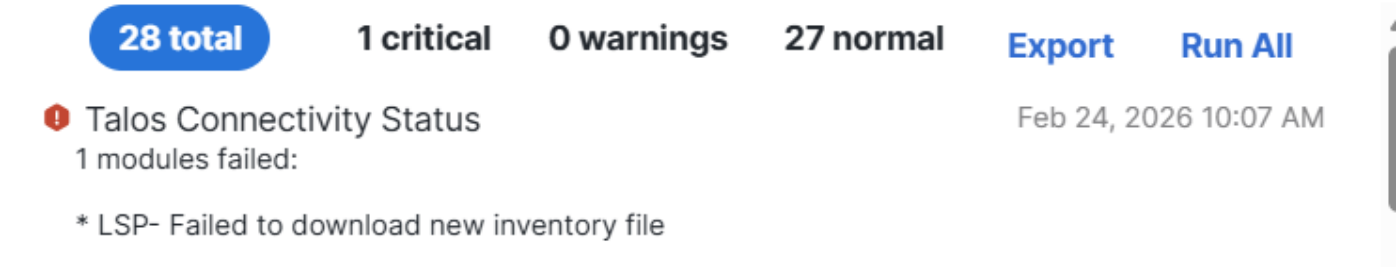
FMC 자동 LSP 업데이트 "새 인벤토리 "을(를) 다운로드하지 못했습니다

문제

Cisco FMC에서 자동 LSP(Lightweight Security Package) 업데이트가 실패했습니다. 수동 LSP 설치가 계속 제대로 작동하는 동안 LSP 업데이트가 더 이상 자동으로 설치되지 않습니다. VDB 업데이트 및 Snort 규칙 업데이트는 자동 프로세스를 통해 정상적으로 작동합니다.

알림 예



inline_image_0.png

환경

- Cisco Secure Firewall Firepower Management Center 7.6.x On-Prem(모든 FMC 모델 및 버전 7.6 이상에 적용)

해결

자동 LSP 업데이트 실패를 해결하려면 업데이트 프로세스를 차단할 수 있는 업스트림 방화벽 또는 네트워크 디바이스에서 필요한 네트워크 연결이 올바르게 구성되었는지 확인합니다.

1: 현재 LSP 버전 상태 확인

firepower Threat Defense 디바이스에 설치된 현재 LSP 버전을 확인합니다.

```
show version
```

현재 LSP 버전을 보여주는 출력 예:

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

모델: Cisco Secure Firewall 3140 Threat Defense(80) 버전 7.6.2.1(빌드 3)

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

LSP 버전: lsp-rel-20260121-2008

VDB 버전: 421

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

2: 네트워크 연결 요구 사항 확인

다음과 같은 대상에 대해 업스트림 방화벽 또는 네트워크 보안 디바이스에서 포트 80을 통한 아웃바운드 액세스가 허용되는지 확인합니다.

- updates-dyn-talos.sco.cisco.com - LSP 업데이트에 필요
- updates.ironport.com - 보안 콘텐츠 업데이트에 필요

이러한 대상은 자동 업데이트 프로세스가 제대로 작동하기 위해 필수적입니다. 이러한 연결을 차단하면 자동 LSP 업데이트가 차단되는 동시에 수동 업데이트가 작동합니다.

오류가 있는 FMC의 연결 테스트 예

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

<h1>웹 페이지 차단됨</h1>
```

방문하려는 웹 페이지가 회사 정책에 따라 차단되었습니다. 오류라고 생각되면 시스템 관리자에게 문의하십시오.

/var/log/sf/talos_agent.log의 오류 로그 예

sf/talos_agent.log:TalosAgent:오류:
updater.go:talosagent.cisco.com/pkg/updater.UpdateService:475 2026/02/13 04:11:05 Failed to downloac
오류: 코드 = 내부 desc = http 오류 503 파일을 다운로드하는 동안 서비스를 사용할 수 없음
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
실패: 연결 오류: 피어별 연결 재설정(os 오류 104)

3: 업데이트 구성 확인

LSP 업데이트를 위한 방화벽 관리 센터에 자동 업데이트가 올바르게 구성되어 있는지 확인합니다. VDB 및 Snort 규칙 업데이트가 자동으로 계속 작동한다는 사실은 기본 업데이트 메커니즘이 작동하지만 LSP 관련 연결을 차단할 수 있음을 의미합니다.

4: 연결 테스트

필요한 대상이 업스트림 보안 디바이스를 통해 액세스할 수 있는지 확인한 후 자동 업데이트 프로세스를 모니터링하여 LSP 업데이트가 정상 운영을 재개하는지 확인합니다.

작업 출력의 예

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

* 시도 208.90.58.25:80...

* updates.ironport.com(208.90.58.25) 포트 80(#0)에 연결됨

> GET/HTTP/1.1

> 호스트: updates.ironport.com

> 사용자 에이전트: curl/7.79.1

> 수락: */*

>

* 번들을 다중 사용을 지원하지 않는 것으로 표시

< HTTP/1.1 200 정상

< 서버: nginx/1.20.1

< 날짜: 월, 2026년 3월 16일 20:22:35 GMT

< Content-Type: text/html

< Content-Length: 689

< 최종 수정일: 2006년 9월 6일 수요일 17:26:12 GMT

< 연결: 연결 유지

< ETag: "44ff04b4-2b1"

< 만료: 2026년 3월 17일 화요일 20:22:35 GMT

< Cache-Control: max-age=86400

< 허용 범위: 바이트

<

<HTML>

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

  <헤드>

```
  </HEAD>

  <본문>

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

    <P>

      IronPort 업데이트 서버입니다. 새 파일을 다운로드하려는 경우

traffic monitor, merlin 또는 WBRS 패키지에서 이 페이지에 오류가 발생했습니다.

  다운로드 지침은 Update Manager 릴리스 정보를 참조하십시오

새로운 소프트웨어.

    </P>

    <P>

      문의 사항이 있는 경우 언제든지 IronPort 고객 관리 팀에 문의하십시오.

      (877)641-4766 또는 <A HREF="mailto:support@ironport.com">support@ironport.com</A>에서 확인할
수 있습니다.

    </P>

  </BODY>

</HTML>

* host updates.ironport.com에 대한 연결 #0 그대로 유지
```

장치가 Cisco 공용 문서에 명시된 기타 다양한 업데이트 및 다운로드 유형에 대한 포트 및 도메인 연결에 필요한 요구 사항을 준수하는지 확인합니다.

- Cisco Secure Firewall Management Center 관리 가이드, 7.6: 보안, 인터넷 액세스 및 통신 포트

원인

자동 LSP 업데이트 실패는 필요한 업데이트 서버에 대한 네트워크 연결이 차단되어 발생합니다. 특히 updates-dyn-talos.sco.cisco.com 및 updates.ironport.com에 대한 포트 80을 통한 아웃바운드 액세스가 업스트림 방화벽 규칙 또는 네트워크 보안 정책에 의해 제한되고 있습니다. 따라서 FMC에서 LSP 업데이트를 자동으로 다운로드하고 설치할 수 없으며 다른 다운로드 방법 또는 캐시된 콘텐츠를 사용할 수 있으므로 수동 업데이트를 계속 수행할 수 있습니다.

그러나 FMC가 Cisco 클라우드 사이트에서 대용량 파일을 다운로드하는 기능에 의해서도 문제가 발생할 수 있습니다. FMC 대역폭을 줄이고 동일한 시간 내에 다른 여러 소프트웨어 업데이트(예: SRU 및 VDB)를 함께 사용하면 대역폭 경쟁이 발생하여 다운로드가 실패할 수 있습니다. 이러한 경우 소프트웨어 다운로드 시간을 분리하여 다운로드에 필요한 대역폭을 충분히 확보하거나 업스트림 대역폭 문제를 해결하십시오.

관련 콘텐츠

- Cisco 기술 지원 및 다운로드
- Cisco Secure Firewall Management Center 관리 가이드, 7.6: 보안, 인터넷 액세스 및 통신 포트

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.