7.4.3에서 7.6.4로 업그레이드한 후 FTD 관리 인터페이스 오류

목차

문제

Cisco Secure Firewall 3130 FTD(Threat Defense) HA(High Availability) 쌍을 버전 7.4.3에서 7.6.4로 업그레이드한 후 기본 유닛이 FMC(Firewall Management Center)에서 99% 완료되었지만 응답이 없는 것으로 나타났습니다. 보조 유닛이 성공적으로 업그레이드되고 HA 쌍에서 액티브 상태가 되었습니다. 기본 유닛이 SSH 연결에 응답하지 않아 FMC가 해당 유닛과 통신할 수 없습니다.

조사 결과, FXOS에서 다음과 같은 중대한 결함이 발견되었습니다.

```
Critical  F1000398 2026-08-14T20:52:06.297     58437 [FSM:FAILED]: out-of-band interface configuration(
```

FTD 업그레이드 로그에 업그레이드가 실제로 성공적으로 완료되었지만(100% 완료) SFTunnel 서비스가 제대로 시작되지 않아 FTD와 FMC 간의 통신이 차단되었습니다. 디바이스는 자체, 게이트웨이, 피어 FTD 유닛을 ping할 수 있지만 다른 서브넷에 상주하는 FMC에 연결할 수 없습니다.

환경

- Cisco Secure Firewall 3130 Threat Defense HA 쌍
- 원본 소프트웨어 버전: FTD 7.4.3
- 대상 소프트웨어 버전: FTD 7.6.4(빌드 69)
- Cisco FX-OS(Extensible Operating System) v2.16.1(빌드 147)
- 고정 IP 주소 지정으로 구성된 관리 인터페이스
- FTD 관리 네트워크와 다른 서브넷에 있는 FMC 서버

해결

영향을 받는 FTD 유닛의 관리 인터페이스를 완전히 재구성하여 문제가 해결되었습니다. 다음 단계를 수행했습니다.

1단계: SSH가 작동하지 않았으므로 콘솔 액세스를 통해 FTD에 연결합니다.

2단계: 업그레이드 로그를 확인하여 업그레이드 완료 상태를 확인합니다.

```
root@device:/ngfw/var/log/sf/Cisco_FTD_SSP_FP3K_Upgrade-7.6.4# cat status.log
```

3단계: FXOS의 관리 인터페이스 결함을 확인합니다.

```
device# show fault
```

4단계: 관리 IP 주소를 재구성하여 기본적인 트러블슈팅을 시도합니다(이렇게 해도 문제가 해결되지 않음).

5단계: 콜드 재부팅을 수행합니다(이렇게 해도 문제가 해결되지 않음).

6단계: FTD CLI에서 management0 인터페이스를 완전히 비활성화합니다.

```
configure network management-interface disable management0
```

7단계: management0 인터페이스를 다시 활성화합니다.

```
configure network management-interface enable management0
```

8단계: 관리 인터페이스에 대한 네트워크 설정을 다시 구성합니다.

```
configure network ipv4 manual <ip_address> <netmask> <gateway>
```

9단계: FXOS 알림이 지워졌는지 확인하고 FTD에서 이제 FMC를 ping할 수 있는지 확인합니다.

```
root@device:/# ping <FMC_IP_address>
```

10단계: manage_procs.pl 스크립트를 사용하여 SFTunnel 서비스를 다시 시작합니다.

```
manage_procs.pl restart sftunnel
```

11단계: SFTunnel 연결 확인:

```
root@device:/# sftunnel_status.pl
```

12단계: HA 작업이 올바르게 작동하는지 확인하기 위해 장애 조치 기능을 테스트합니다.

이 단계를 완료한 후 FTD는 FMC와 제대로 통신할 수 있었으며 모든 연결 및 장애 조치 테스트에 성공했습니다. 그런 다음 핫픽스 업그레이드를 문제 없이 적용할 수 있습니다.

원인

7.4.3에서 7.6.4로 FTD를 업그레이드한 후 업그레이드 프로세스가 성공적으로 완료되었음에도 관리 인터페이스가 제대로 초기화되지 않은 것이 근본 원인입니다. 업그레이드 프로세스 중에 대역외 관리 인터페이스 FSM(Configuration Finite State Machine)이 실패하여 관리 인터페이스가 올바른 연결을 설정하지 못했습니다. 이 동작은 Cisco 버그 ID CSCww08417에 설명되어 있습니다.

이 문제는 이전에 보고된 결함 Cisco 버그 ID CSCwj04154 및 Cisco 버그 ID CSCwa69303과 유사하지만 다른 조건에서 발생합니다. 실제로 업그레이드가 성공적으로 완료되었으나 관리 연결이 끊어진 경우, 관리 인터페이스 장애가 99% 완료되었을 때 업그레이드 실패라는 잘못된 인상을 주었습니다.

관련 콘텐츠

- Cisco 버그 ID CSCww08417 - 업그레이드 후 FTD 관리 인터페이스가 시작되지 않을 수 있습니다.
- Cisco Secure Firewall Threat Defense 호환성 가이드
- Cisco 기술 지원 및 다운로드

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.