맞춤형 정책 탐지로 인해 FTD 업그레이드 중에 Snort 엔진 업그레이드가 차단됨

목차

문제

FMC에서 관리하는 HA FPR-4115에서 버전 7.2에서 7.4.4로 FTD를 업그레이드하는 동안 Snort 3으로의 Snort 엔진 업그레이드가 차단되며, Snort 2 사용자 지정 규칙을 변환하지 못하거나 사용자 지정 침입 또는 네트워크 분석 정책을 사용하지 못한다는 오류 메시지가 표시됩니다. 특정 오류 메시지 상태: "Snort 3으로 업그레이드할 수 없습니다. 디바이스에서 하나 이상의 사용자 지정 침입 정책 또는 네트워크 분석 정책을 사용합니다." 더 자세한 오류 메시지는 Snort 2 사용자 지정 규칙을 변환할 수 없음을 나타내며 자세한 내용은 /var/sf/htdocs/ips/snort.rej을 참조하십시오. 문제는 이 오류가 Snort 3으로의 마이그레이션을 막고 검사 기능에 영향을 미치는지 여부입니다.

환경

- Cisco Secure Firewall Firepower 버전 7.3
- FMC(firepower Management Center) 버전 7.7.11
- HA(High Availability) 컨피그레이션의 FTD 디바이스
- 하드웨어: FPR-4115
- 업그레이드 경로: FTD 7.2~7.4.4
- 업그레이드 전 최신 버전의 VDB
- Objects > Intrusion Rules > Snort 2 All Rules is empty 아래의 Local Rules 섹션

해결

Snort 엔진 업그레이드를 차단하는 오류 메시지는 Cisco 버그 ID CSCwn46794과 관련된 동작을 문서화하며, 실제 맞춤형 Snort 2 규칙이 없는 경우 기능 차단기를 나타내지 않습니다.

확인 단계

1단계: 사용자 지정 Snort 2 규칙 상태 확인

FMC 인터페이스로 이동하여 맞춤형 Snort 2 규칙을 확인합니다.

`Objects(개체) > Intrusion Rules(침입 규칙) > Snort 2 All Rules(Snort 2 모든 규칙) > Local Rules(로컬 규칙)`

2단계: VDB 버전 확인

업그레이드를 진행하기 전에 VDB(취약성 데이터베이스)가 최신 버전인지 확인하십시오.

3단계: 오류 세부사항 검토

참조된 파일에서 자세한 오류 정보를 확인합니다.

```
/var/sf/htdocs/ips/snort.rej
```

업그레이드 프로세스

"로컬 규칙" 섹션이 비어 있는 것으로 확인되면(사용자 지정 Snort 2 규칙이 존재하지 않음) 오류 메시지에도 불구하고 업그레이드를 진행할 수 있습니다. 차단 오류는 이 시나리오에서 오탐이며 변환이 필요한 실제 사용자 지정 규칙을 나타내지 않습니다.

1단계: Snort 3 업그레이드 진행

Snort 3 엔진 업그레이드가 포함된 버전 7.4.4로의 FTD 업그레이드 프로세스를 계속 진행합니다.

2단계: 업그레이드 후 검증

업그레이드가 성공적으로 완료되면 트래픽 플로우를 테스트하여 Snort 3 엔진을 통해 예상되는 동작을 확인합니다.

3단계: 시스템 성능 모니터링

새로운 Snort 3 엔진에서 검사 기능이 예상대로 작동하는지 확인합니다.

원인

업그레이드 차단 메시지는 Cisco 버그 ID CSCwn46794과 관련된 동작을 문서화합니다. 이 버그로 인해 변환이 필요한 실제 사용자 지정 Snort 2 규칙이 없는 경우에도 시스템이 사용자 지정 침입 정책 또는 네트워크 분석 정책에 대한 오류 메시지를 표시합니다. 로컬 규칙 섹션이 비어 있는 경우 오류 메시지가 오탐으로 표시되지만, 시스템 업그레이드 전 유효성 검사에서 사용자 지정 정책의 존재를 잘못 식별합니다.

관련 콘텐츠

- Cisco 버그 ID CSCwn46794
- Cisco 버그 ID CSCwk07199
- 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.