FMC에서 VDB 업데이트 프로세스 확인

목차

문제

관리자는 VDB(Vulnerability Database) 업데이트를 실행할 때 VDB 업데이트가 누적되는지, 그리고 중간 버전을 건너뛸 수 있는지 파악해야 합니다.

이 예에서는 VDB 버전 393에서 버전 427로 업데이트할 때 문제가 발생합니다. 특히, 여러 업그레이드 단계가 필요한지 또는 직접 업그레이드 경로가 지원되는지 여부가 불확실합니다. 또한 VDB 업데이트 및 후속 정책 구축 프로세스 중에 서비스가 중단될 수 있다는 우려도 제기됩니다.

환경

- FMC(Secure Firewall Management Center) 소프트웨어 버전 7.4.2.4. 다른 소프트웨어 버전도 영향을 받습니다.
- FPR 2110의 FTD(Firewall Threat Defense). 다른 하드웨어 플랫폼도 영향을 받습니다.
- 현재 VDB 버전: 393. 다른 소프트웨어 버전도 영향을 받습니다.
- 대상 VDB 버전: 427. 기타 소프트웨어 버전도 영향을 받습니다.

해결

FMC의 VDB 업데이트는 누적되므로 중간 단계 없이 이전 버전에서 최신 버전으로 직접 업그레이드할 수 있습니다.

VDB 업데이트 프로세스

중간 VDB 업그레이드 단계 없이 VDB 버전 393에서 VDB 버전 427로 직접 업데이트할 수 있습니다. VDB 버전 357부터 Cisco는 FMC 플랫폼에 기본 VDB까지 모든 VDB 버전 설치를 지원합니다.

최신 VDB 버전을 다운로드하려면 Cisco Software Download Center(https://software.cisco.com/download/home/286332319/type/286321931/release/VDB)로 이동합니다

서비스 영향 고려 사항

기본 위험은 FMC의 VDB 설치 자체와는 관련이 없으며 VDB 업데이트 후 FTD의 첫 번째 정책 구축과도 관련이 있습니다. 대부분의 경우 VDB 업데이트 후 첫 번째 구축은 Snort 프로세스를 다시 시작하며, 이는 트래픽 검사를 일시적으로 중단합니다.

이 중단 기간 중:

- 트래픽은 추가 검사 없이 삭제 또는 통과될 수 있습니다.
- 구체적인 동작은 프로세스 재시작 중에 트래픽을 처리하도록 FTD가 구성되는 방식에 따라 달라집니다.

모범 사례 권장 사항:

- 계획된 유지 관리 기간 중에 정책 구축 부분을 예약합니다.
- 사용자의 영향을 최소화하기 위해 네트워크 운영과 협력
- 구축 프로세스 중 및 후에 시스템 상태를 모니터링합니다.

원인

- VDB 357부터 FMC의 기본 VDB까지 모든 VDB 업데이트를 설치할 수 있습니다.
- 설치하려면 새 취약성 서명을 활성화하기 위해 정책을 재배포해야 합니다. 그러면 관리되는 FTD 디바이스에서 Snort 프로세스가 다시 시작됩니다. 이렇게 다시 시작하면 새 데이터베이스가 로드되고 검사 엔진이 다시 초기화되는 동안 트래픽 검사 기능이 잠시 중단됩니다.

관련 콘텐츠

- Cisco Secure Firewall Management Center 관리 설명서 - 시스템 업데이트
- Cisco Secure Firewall Management Center 디바이스 컨피그레이션 가이드 - 구축
- 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.