보안 방화벽 FTD 비밀번호 재설정(&N)

문제

로컬 관리자 비밀번호가 손실되어 CLI를 통해 FTD(Firewall Threat Defense)에 액세스할 수 없습니다. 관리 목적으로 해당 노드에 액세스할 수 없습니다. 초기에는 관리자 비밀번호가 기본값에서 변경되었으며 알 수 없는 것으로 간주되어 액세스 및 기본 자격 증명을 복원하기 위해 공장 초기화(reimage)를 완료해야 하는 문제가 발생했습니다. 이 상황을 처리하는 적절한 절차에 대해 구체적인 의문이 제기되었습니다.

환경

- Cisco Secure Firewall 1000, 2100 및 3100 FTD 매니지드 Firepower 관리 센터

해결

더 복잡한 리이미지 절차를 진행하기 전에 기본 관리자 자격 증명을 사용하여 영향받는 FTD 디바이스에 액세스를 시도하는 것과 관련된 해상도입니다.

1: 시작하기 전에 공장 기본 관리자 자격 증명을 사용하여 영향받는 FTD 디바이스에 로그인을 시도합니다.

```
Username: admin
Password: Admin123
```

이 단계를 먼저 수행해야 합니다. 이 단계를 수행하면 좀 더 번거로운 복구 절차가 필요하지 않게 될 수 있습니다.

2: 기본 자격 증명이 제외된 경우 표준 FTD CLI 비밀번호 변경 절차를 통해 관리자 비밀번호를 알려진 새로운 값으로 재설정합니다.

이미지로 다시 설치 프로세스: Cisco Secure Firewall ASA 및 Threat Defense 리이미지 가이드

- Cisco 설명서의 단계에 따라 영향을 받는 FTD 디바이스를 완전히 재이미지화합니다.
- 이미지로 다시 설치 과정을 통해 공장 기본 자격 증명을 복원합니다.

원인

근본 원인은 영향을 받는 FTD 디바이스의 관리자 비밀번호가 초기 구축 과정에서 공장 기본값에서 변경된 적이 없었기 때문입니다. 액세스 손실은 실제 자격 증명 손실이 아니라 비밀번호를 알 수 없다는 잘못된 가정 때문이었습니다. 인시던트 전반에 걸쳐 기본 관리자 자격 증명을 사용하여 디바이스에 계속 액세스할 수 있었습니다.

관련 콘텐츠

- 고가용성을 보장하는 보안 방화벽 위협 방어의 결함 있는 유닛 교체
- 방화벽 위협 방어를 위한 Cisco FXOS 트러블슈팅 가이드: 이미지 관리
- Cisco Secure Firewall ASA 및 Threat Defense 리이미지 가이드
- firepower 디바이스 등록 구성, 확인 및 문제 해결
- Firepower 어플라이언스에서 FTD 고가용성 설정
- 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.