SysPrep 골든 이미지를 사용하여 보안 액세스 구축에서 중복된 ZTNA 디바이스 ID 확인

목차

문제

SysPrep 골든 이미지에서 배포된 여러 Windows 물리적 시스템이 여러 엔드포인트에서 동일한 ZTNA 디바이스 ID, 특히 동일한 ztnaDeviceId를 생성하고 있습니다. 이러한 중복으로 인해 다음과 같은 몇 가지 중요한 문제가 발생합니다.

- 동일한 ZTNA 장치 ID로 반복해서 장치 재등록
- 각 재등록 프로세스 중 공개 키 덮어쓰기
- 가장 최근에 등록된 디바이스를 제외한 모든 머신의 상태 확인 실패
- 영향을 받는 엔드포인트에 대한 보안 액세스를 통한 액세스 실패

관찰된 동작은 플릿의 여러 시스템이 동일한 ZTNA 장치 ID를 공유할 때 발생하며, 각 등록이 이전 시스템의 공개 키를 덮어쓰게 됩니다. 등록할 최신 시스템을 제외한 모든 시스템은 보안 상태 검사를 전송하지 못하므로 Secure Access 인프라를 통한 액세스가 거부됩니다.

여러 호스트 이름 및 사용자 ID 쌍이 동일한 ZTNA 디바이스 ID에 연결된 것으로 식별되어 구축 전반에서 복제 문제의 범위를 확인할 수 있습니다.

환경

- Cisco Secure Access(ZTNA 구현)
- Windows 물리적 컴퓨터(가상 컴퓨터 아님)
- SysPrep 골든 이미지 구축 방법론
- 이미지 배포를 위한 Windows ADK(평가 및 배포 키트) 도구

- 이미지 캡처용 ESD(Electronic Software Delivery) 파일 형식
- 필수 소프트웨어 설치를 포함한 표준화된 OS 강화 프로세스
- 표준 로컬 관리자 및 게스트 계정 컨피그레이션

해결

해결 과정에는 종합적인 로그 분석과 세부 조사를 통한 근본 원인 규명이 수반되었다.

근본 원인 파악 및 해결

조사 결과, SysPrep 프로세스에서 골든 이미지 구축 과정에서 고유 디바이스 식별자를 제대로 생성하지 못한 것으로 나타났습니다.

관련 분석:

특히 Windows 레지스트리 키를 검사합니다.

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion
```

다음을 사용하여 사용자 보안 식별자 정보 수집:

```
whoami /user
```

이 확인 과정에서 SysPrep 프로세스를 수정하여 디바이스별 식별자가 배포 중에 올바르게 다시 생성되도록 하여 여러 물리적 머신에서 ZTNA 디바이스 ID가 중복되지 않도록 해야 했습니다.

- dartcli.exe -nu 명령을 실행하여 UDID를 갱신하면 "HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Cisco\Cisco Secure Client\DeviceDetails" 레지스트리 경로에서 Nunce 값이 변경됩니다.
- C:\ProgramData\Cisco\Cisco Secure Client\ZTA\enrollments에서 JSON 파일을 삭제하고 ZTA 서비스를 다시 시작하면 사용자 등록이 취소됩니다. 사용자를 수동으로 등록해야 합니다

. 이렇게 하면 다른 영향 없이 새 JSON 파일이 생성됩니다.

- 모든 서버에서 값을 확인/평가하지 않는 한 모든 엔드포인트에서 UDID를 갱신하는 것은 어떤 영향도 미치지 않아야 합니다.

1. 관리자로 명령 프롬프트를 시작하고 "%ProgramFiles(x86)%\Cisco\Cisco Secure Client\DART" 디렉토리로 이동합니다.

2. dartcli.exe -u를 실행하여 현재 UDID의 값을 확인합니다.

3. dartcli.exe -nu 명령을 실행합니다. 이 명령은 UDID를 갱신합니다.

4. 2단계의 명령을 반복하여 새 값을 확인합니다.

5. C:\ProgramData\Cisco\Cisco Secure Client\ZTA\enrollments 디렉토리에서 JSON 파일을 삭제합니다.

6. VPN 및 ZTA 서비스를 다시 시작합니다. 이 시점에서 ZTA는 등록되지 않은 상태여야 합니다.

7. 사용자가 ZTA를 수동으로 등록하도록 허용

9. JSON 파일에서 새 ztnaDeviceId 값을 확인합니다.

모니터링 및 검증

고유한 ZTNA 장치 ID 생성을 보장하기 위해 교정 조치를 구현한 후:

- 여러 시스템에서 등록 프로세스 모니터링
- 각 컴퓨터에서 고유한 ZTNA 장치 ID를 생성했는지 확인했습니다.
- 등록된 모든 디바이스에서 성공적인 상태 확인 기능 확인
- 등록 중에 공개 키 덮어쓰기가 더 이상 발생하지 않았음을 확인했습니다.

원인

SysPrep 골든 이미지 배포 프로세스에서 ZTNA 등록을 위한 고유 디바이스 식별자를 제대로 생성하지 못함에 따라 근본 원인이 식별되었습니다. 동일한 SysPrep 골든 이미지에서 여러 Windows 물리적 시스템을 구축하는 경우 ZTNA 디바이스 ID를 생성하는 데 사용되는 특정 디바이스별 식별자는 구축된 모든 시스템에서 동일하게 유지됩니다.

SysPrep 프로세스는 OS 컨피그레이션 및 소프트웨어 구축 표준화에 효과적이지만 Cisco Secure Client가 고유한 ZTNA 디바이스 ID를 생성하기 위해 사용하는 특정 식별자를 재생성하도록 구성되지 않았습니다. 그 결과 동일한 골든 이미지에서 구축된 모든 시스템이 동일한 ZTNA 디바이스 식별 매개변수를 상속받아 Secure Access 인프라에서 등록 충돌 및 인증 실패가 발생했습니다.

관련 콘텐츠

- 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.