

ISE 관리자 GUI 로그인시 PingID 페더레이션 RADIUS 토큰으로 실패

목차

문제

PingID 페더레이션을 RADIUS 토큰으로 사용하는 경우 Ping 페더레이트가 액세스 수락 응답을 반환한다는 패킷 캡처에도 불구하고 Cisco ISE에 대한 관리자 GUI 로그인이 실패합니다. RADIUS 인증이 네트워크 관점에서 성공적으로 나타나도 로그인 실패가 발생하여 ISE 인터페이스에 대한 관리 액세스가 차단됩니다. 네트워크 패킷 분석을 통해 PingID 서버(10.32.154.200)가 ISE(10.2.200.241)에 예상 Access-Accept 응답을 전송하지만 ISE 관리자 로그인 프로세스가 여전히 성공적으로 완료되지 않음을 확인합니다.

환경

- Cisco ISE(Identity Services Engine) 버전 3.3 패치 7
- 4노드 VM 구축
- RADIUS 토큰 인증으로 구성된 PingID 페더레이션
- ISE IP 주소: 10.2.200.241
- PingID 서버 IP 주소: 10.32.154.200
- 관리 > 관리 액세스에 검토된 관리자 액세스 구성

해결

성공적인 관리자 로그인 기능을 활성화한 해결 방법을 적용하여 문제를 해결했습니다. 다음 섹션에서 설명하는 단계를 수행하여 문제를 해결했습니다.

1단계: 증거 수집 및 분석

ISE와 PingID 서버 간의 RADIUS 인증 흐름을 확인하기 위해 패킷 캡처 증거를 수집하고 분석했습니다. 분석 결과 Ping 페더레이트가 Access-Accept 응답을 올바르게 보낸 것이 확인되었습니다.

2단계: prrt-server.log의 증거

###

prrt-server.log

```
RadiusTokenIDStore,2026-03-27 13:25:04,534,DEBUG,0x7f4942ebb700,cntx=0180887321,sesn=SIT2194/554866250/  
RadiusClient,2026-03-27 13:25:04,534,DEBUG,0x7f4942ebb700,cntx=0180887321,sesn=SIT2194/554866250/183397  
RadiusClient,2026-03-27 13:25:05,074,DEBUG,0x7f490d6b9700,NIL-CONTEXT,onProcessResponse: Processing Res  
RadiusClient,2026-03-27 13:25:05,074,WARN ,0x7f49444c6700,cntx=0180887321,sesn=SIT2194/554866250/183397
```

###

3단계: 메시지 인증자란 무엇입니까?

Message-Authenticator는 네트워크 디바이스와 RADIUS 서버 간에 교환되는 메시지의 무결성 및 신뢰성을 보장하기 위해 RADIUS 패킷에서 사용되는 보안 특성입니다. 공유 비밀 키를 사용하여 전체 RADIUS 패킷에 대해 HMAC-MD5를 사용하여 계산한 암호화 서명입니다. 이 특성은 RADIUS 메시지, 특히 EAP(Extensible Authentication Protocol) 인증 플로우와 관련된 메시지의 변조 및 스푸핑을 방지하는 데 도움이 됩니다.

4단계: 해결 방법 구현

"응답에 메시지 인증자 필요" 비활성화: 관리 / 신원 관리 / 외부 ID 소스 / RADIUS 토큰. RADIUS 토큰 이름을 클릭 한 다음 인증으로 이동 합니다. "응답에 메시지 인증자 필요"의 선택을 취소합니다.

5단계: 검증 테스트

해결 방법을 적용한 후 해결 방법을 확인하기 위해 관리자 로그인 테스트가 실행되었습니다. 이러한 테스트에서는 PingID 페더레이션을 RADIUS 토큰으로 사용하여 ISE 관리 GUI에 대한 액세스 및 인증에 성공한 것을 확인했습니다.

6단계: 모니터링 기간

해결 방법의 안정성을 확보하기 위해 모니터링 및 검증 기간을 설정하였다. 이 기간 동안 오류 또는 오류가 보고되지 않은 상태로 지속적인 관리자 로그인 테스트가 수행되었습니다.

원인

MFA 인증 중에 Cisco ISE 3.3 패치 7과 PingID(Ping Federate) 간의 RADIUS 프로토콜 보안 시행 불일치로 인해 ISE 관리 GUI 로그인 실패가 발생했습니다.

구체적으로,

- Cisco ISE는 외부 RADIUS 토큰 서버의 Access-Accept 응답에 RADIUS 메시지 인증자 특성을 있어야 했습니다.
- PingID가 Message-Authenticator 특성 없이 Access-Accept 응답을 반환했습니다.
- ISE는 응답에 메시지 인증자 필요 설정을 활성화했으므로 인증 자체가 PingID 측에서 성공했지만 RADIUS 응답이 유효하지 않은 것으로 자동 거부되었습니다.
- 이러한 시행은 Cisco ISE의 보안 강화의 일환으로 Blast-RADIUS 취약성(CVE-2024-3596)을 완화합니다.

관련 콘텐츠

- [Blast-RADIUS 프로토콜 스푸핑 완화\(CVE-2024-3596\)](#)

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.