DLP Fail-Closed 동작 구성 - 클라우드 연결 손실 중 사용자 작업 차단

목차

문제

엔드포인트 DLP(EDLP) 모듈이 설치된 사용자는 구성된 EDLP 규칙에 포함되지 않았음에도 불구하고 네트워크 파일 공유에 대한 인쇄 및 복사가 차단되었습니다. 기존의 모든 EDLP 규칙은 해당 규칙에 포함된 특정 사용자 3명만 포함된 MONITOR 모드로 구성되었습니다. 영향을 받은 사용자는 EDLP 시행을 적용하려는 것이 아님에도 불구하고 인쇄 작업 및 파일 공유 복사 작업에 대해 예기치 않은 차단 작업을 경험했습니다.

트러블슈팅 중에 EDLP 클라우드 연결을 사용할 수 없을 때 차단이 발생한 것으로 확인되어 시스템이 장애 조치(fail-closed) 동작을 폴백 메커니즘으로 적용했습니다. EDLP 클라이언트가 정책 판정을 위해 클라우드 서비스에 대한 연결을 설정하지 않은 기간 동안 사용자는 인쇄 거부 및 네트워크 공유 액세스를 경험했습니다.

환경

- Cisco Endpoint DLP module 버전 1.5.0.292
- Cisco Secure Access/Secure/Data Loss Prevention 포털 관리
- 모니터 모드에서 구성된 여러 EDLP 규칙
- 장애 종료 동작으로 구성된 네트워크 공유 채널
- 클라이언트 네트워크 연결에 영향을 주는 DNS 확인 변경

해결

해결책에는 클라우드 연결 손실 시 EDLP 실패 시 닫힘 동작 및 해당 애플리케이션에 대한 이해 및 설명이 포함되었습니다.

근본 원인 분석

DART 번들 및 EDLP 로그를 분석한 결과, 네트워크 공유 채널이 fail-closed로 구성되었기 때문에 EDLP에서 거부 대안을 적용했습니다. 차단 사고 당시 클라이언트 네트워크의 DNS 확인 변경으로 인해 EDLP 클라우드 연결을 사용할 수 없어 시스템이 클라우드 서비스에서 정책 판정을 받지 못했습니다.

Fail-Closed 동작 설명

특정 EDLP 규칙에 사용자 ID가 포함되었는지 여부와 상관없이 EDLP 모듈이 설치되었기 때문에 fail-closed 정책이 사용자 시스템에 적용되었습니다. fail-open/fail-closed 상태는 DLP 정책 컨피그레이션에 프로비저닝된 전역 설정이며, 채널 컨피그레이션은 해당 전역 설정에 따라 적용됩니다.

연결 복구

클라이언트 네트워크에서 DNS 안정성이 복원되면 문제가 자동으로 해결되어 EDLP 클라이언트가 클라우드 서비스에 대한 연결을 다시 설정할 수 있습니다. 기본 네트워크 연결 문제가 해결되면 수동 개입이 필요하지 않습니다.

Fail-Closed 동작을 일으키는 조건

이러한 조건은 EDLP 실패 닫힘 동작을 트리거할 수 있습니다.

- DNS 확인 문제
- 네트워크 중단
- 네트워크 간 스위칭
- 클라이언트와 클라우드 서비스 간의 엔드 투 엔드 연결을 방해하는 모든 조건

원인

네트워크 공유 채널에 대한 EDLP의 실패 닫힘 컨피그레이션으로 인해 차단 동작이 발생했습니다. EDLP 클라이언트가 DNS 확인 변경으로 인해 클라우드 서비스에 대한 연결이 끊기면 정책 판정을 얻을 수 없으므로 구성된 실패-닫힌 동작을 보안 대체 메커니즘으로 시행합니다. 이는 사용자가 EDLP 규칙에 명시적으로 포함되었는지 여부와 상관없이 발생했으며, 클라우드 연결을 사용할 수 없을 때 EDLP 모듈이 설치된 모든 시스템에 장애 종료 설정이 전역적으로 적용되기 때문입니다.

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.