버그 적용 가능성 확인 툴을 사용하여 SD-WAN PSIRT 확인

목차

소개

이 문서에서는 버그 적용 가능성 툴을 사용하여 SD-WAN PSIRT(Product Security Incident Response Team) CVE-2026-20182CSCwt와 관련된 가능한 IoC(Indicators of Compromise)에 대해 admin-tech 파일을 스캔하는 방법에 대해 설명합니다50498

요구 사항

CSCwt50498의 경우 SD-WAN 제어 구성 요소의 admin-tech를 생성해야 합니다. 컨트롤러(vSmart) 관리 기술은 한 번에 하나씩 생성되어야 합니다.

다른 SD-WAN 제어 구성 요소의 admin-techs는 임의의 순서로 생성될 수 있습니다.

Admin-Tech 생성 지침

이러한 파일을 만드는 데 도움이 필요한 경우 다음 문서에서 admin-tech를 생성하는 단계를 참조하십시오. SD-WAN 환경에서 관리 기술을 수집하는 방법.

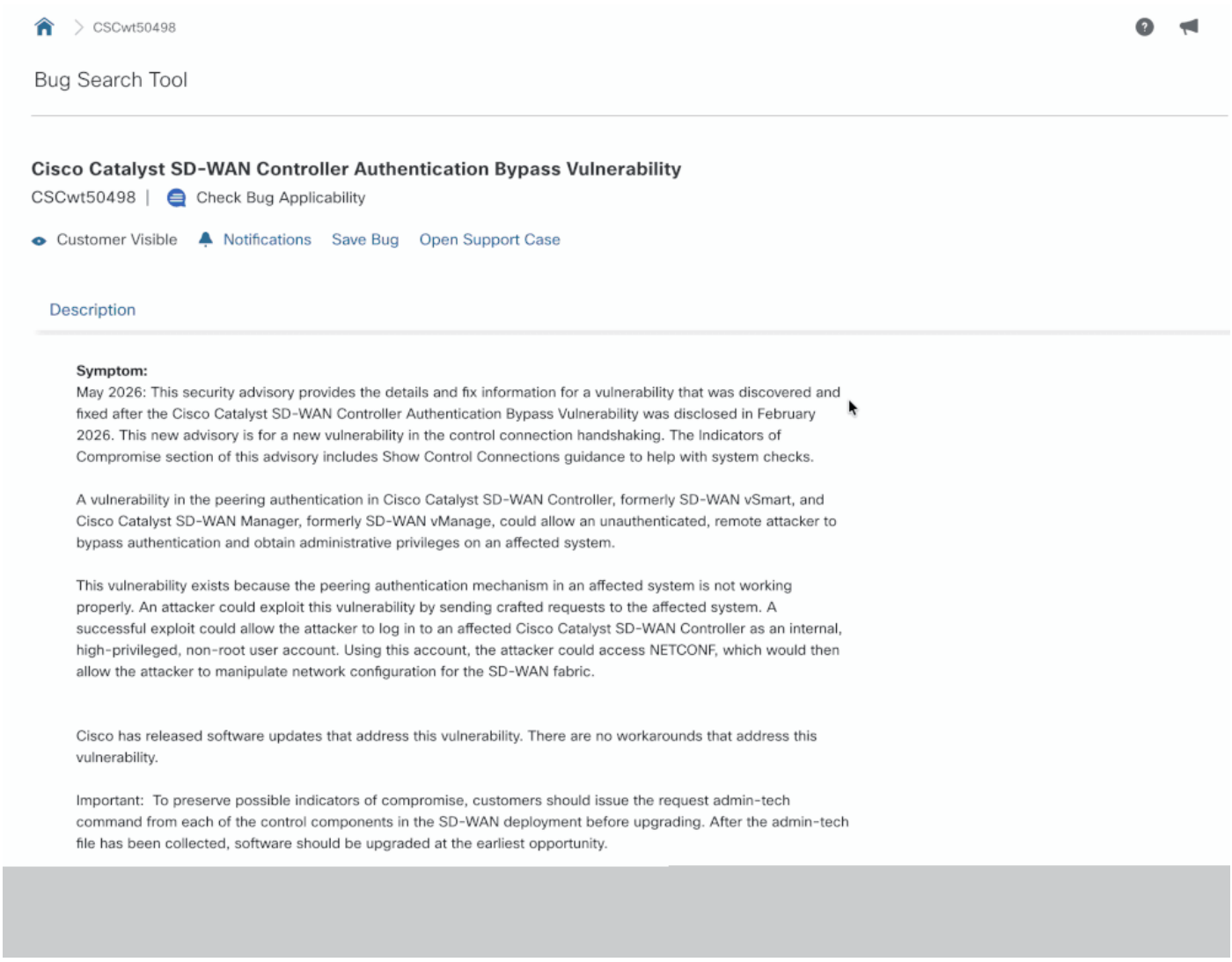
제한 사항

- 파일 크기는 현재 500MB로 제한됩니다.
- 동시 파일 확인은 지원되지 않습니다. 이 도구는 여러 파일을 처리할 수 있지만 한 번에 하나만 처리할 수 있습니다.

사용률

Admin-Tech 확인

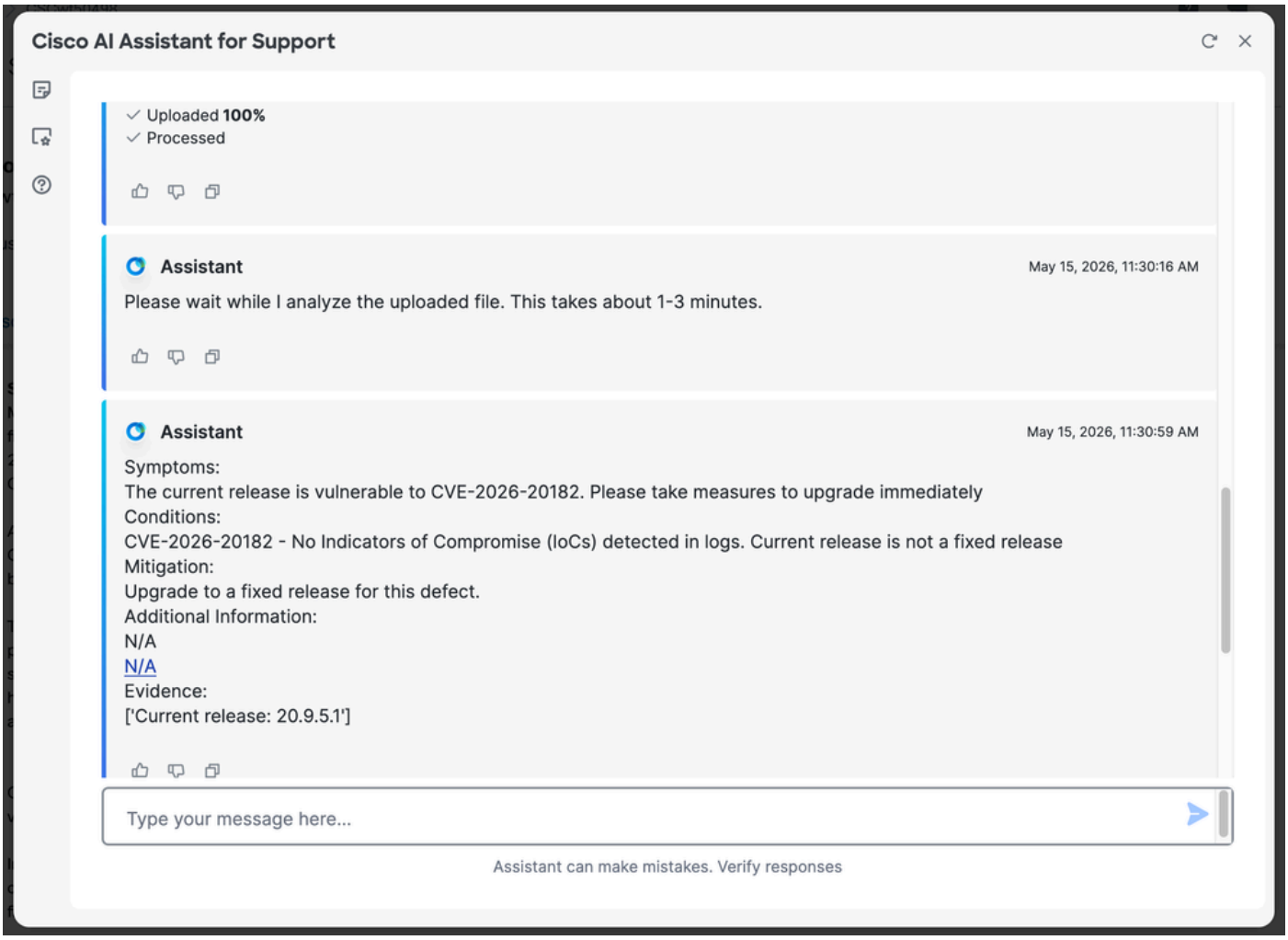
1. 분석할 Cisco Bug ID에 대한 Cisco Bug Search Tool 페이지로 이동합니다.
2. 제목 아래에서 텍스트나 아이콘 "버그 적용 가능성 확인"을 클릭합니다. 팝업 창이 나타납니다.
3. 분석할 admin-tech 파일을 삭제하거나 선택합니다.



결과 - 표시기 없음

지표가 발견되지 않으면 로그에서 "CVE-2026-20182 - No Indicators of Compromise (IoC) detected(CVE-2026-- No Indicators of Compromise (IoC) 탐지)"와 유사한 메시지가 표시됩니다. 현재 릴리스가 고정 릴리스가 아닙니다"가 나타납니다. 메시지는 분석 중인 특정 버그 ID를 참조합니다.

참고: 아직 업그레이드하지 않은 경우 계속 진행하여 수정 사항이 포함된 릴리스로 즉시 업그레이드하십시오.



결과 - 발견된 지표

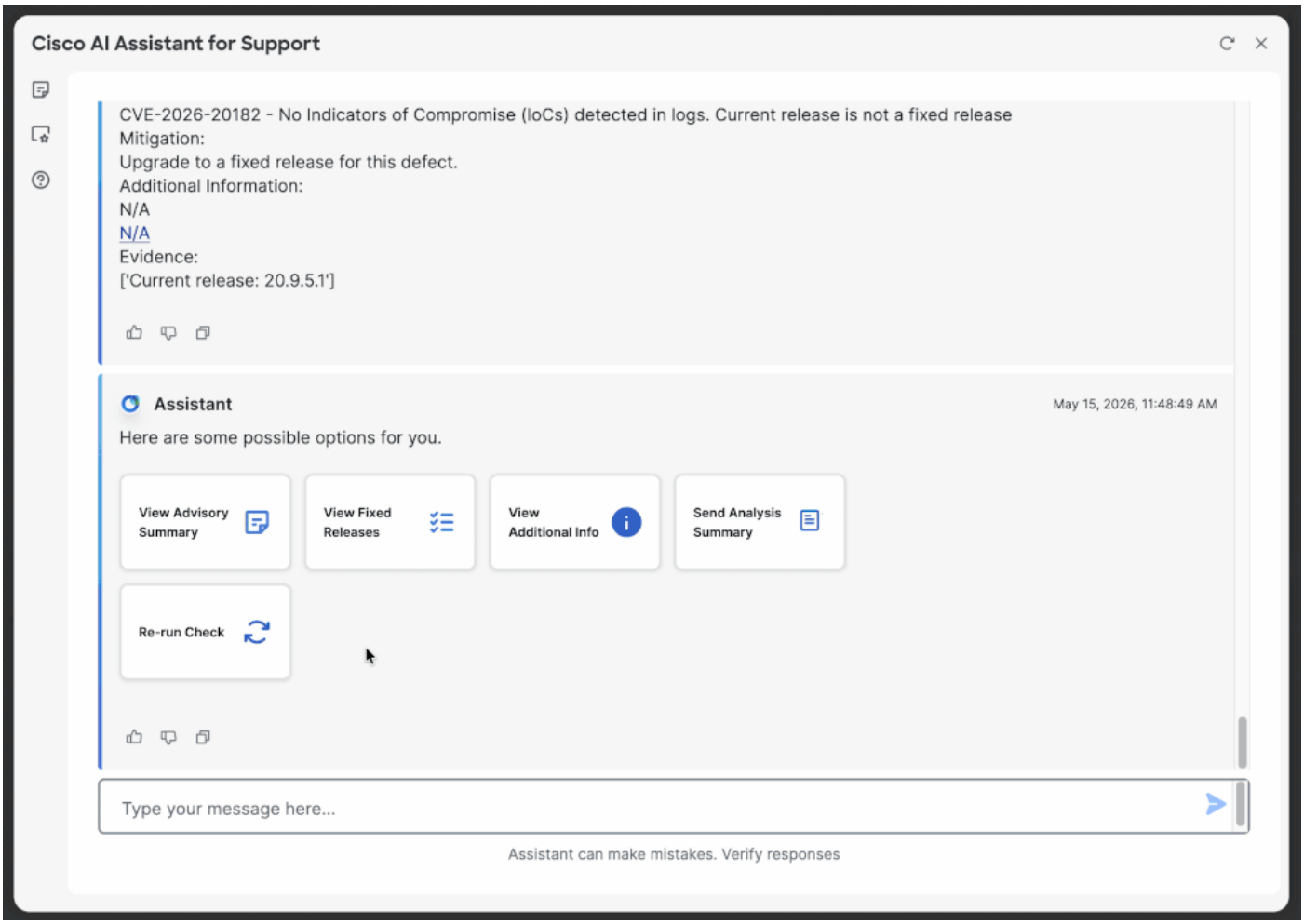
툴에서 지표를 찾으면 "IoC(Potential Indicators of Compromise, 잠재적 IoC) Detected" 메시지가 나타납니다.

추가 수동 검토를 위해 Cisco TAC 케이스를 열고 관리 기술을 업로드하십시오.

참고: 아직 업그레이드하지 않은 경우 계속 진행하여 수정 사항이 포함된 릴리스로 즉시 업그레이드하십시오.

추가 관리 기술 분석

다른 관리 기술을 분석하려면 "Re-run(재실행)"을 클릭하고 해당 Cisco 버그 ID(예: CSCwt50498)를 입력하여 업로드 섹션을 다시 확인합니다. 다른 옵션으로는 위로 스크롤하여 "Check <Bug ID>(버그 ID 확인)"을 클릭하거나 채팅에 버그 ID를 입력하는 방법이 있습니다.



추가 옵션 사용 가능

관리 기술을 분석한 후 다음 추가 옵션을 도구에서 사용할 수 있습니다.

- 권고 사항 요약 보기
- 고정 릴리스 보기
- 추가 정보 보기
- 분석 요약 보내기

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.