보안 엔드포인트에 표시된 취약성 수정

목차

소개

이 문서에서는 엔드포인트에 대한 Cisco 위험 점수를 확인하고 수정을 적용하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco Secure Endpoint 콘솔

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- Secure Endpoint Console v5.4.2025030619

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

문제

Cisco Security Risk Score는 0~100의 척도로 표시됩니다. 기술 심각도와 실제 공격자가 어떻게 야생의 취약성을 활용하고 있는지 살펴봄으로써 취약성의 위험을 정량화합니다.

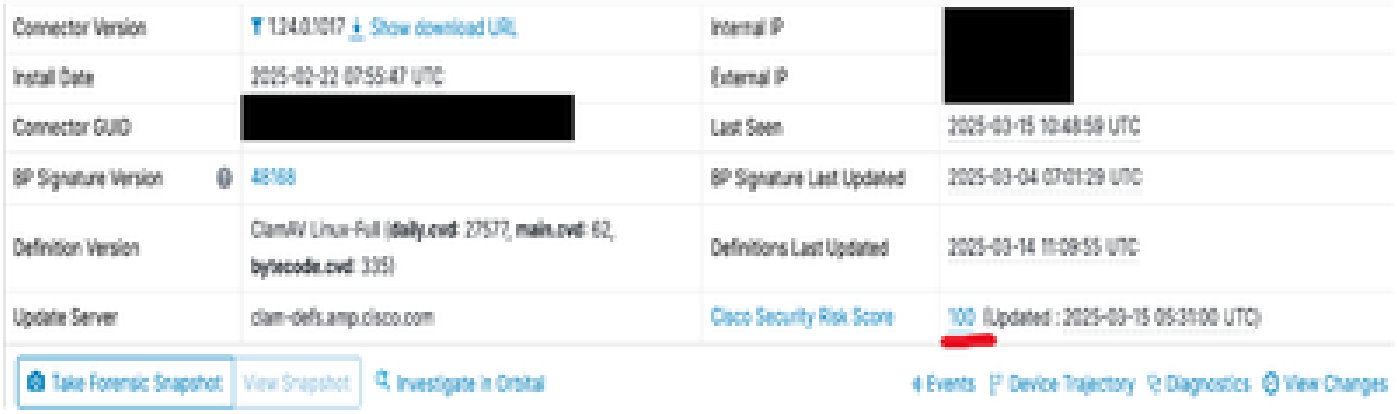
엔드포인트에 대한 Cisco 보안 위험 점수를 확인하고 제안된 수정을 적용합니다.

솔루션

1- Cisco 보안 위험 점수를 보려면 Management(관리) > Computers(컴퓨터)로 이동하여 표시된

Cisco Security Risk Score(Cisco 보안 위험 점수)를 선택합니다.

2- 컴퓨터 목록이 표시됩니다. 확인할 컴퓨터 정보를 확장하고 다음과 같이 표시된 Cisco Security Risk Score(Cisco 보안 위험 점수) 번호를 클릭합니다.



3- 엔드포인트에 영향을 주는 CVE 목록이 표시됩니다. 아래와 같이 Fix Available을 클릭합니다.

4- 아래 표시된 대로 CVE에 대한 권장 수정 사항이 나와 있습니다.

Vulnerability Fixes

CVE-2023-4863

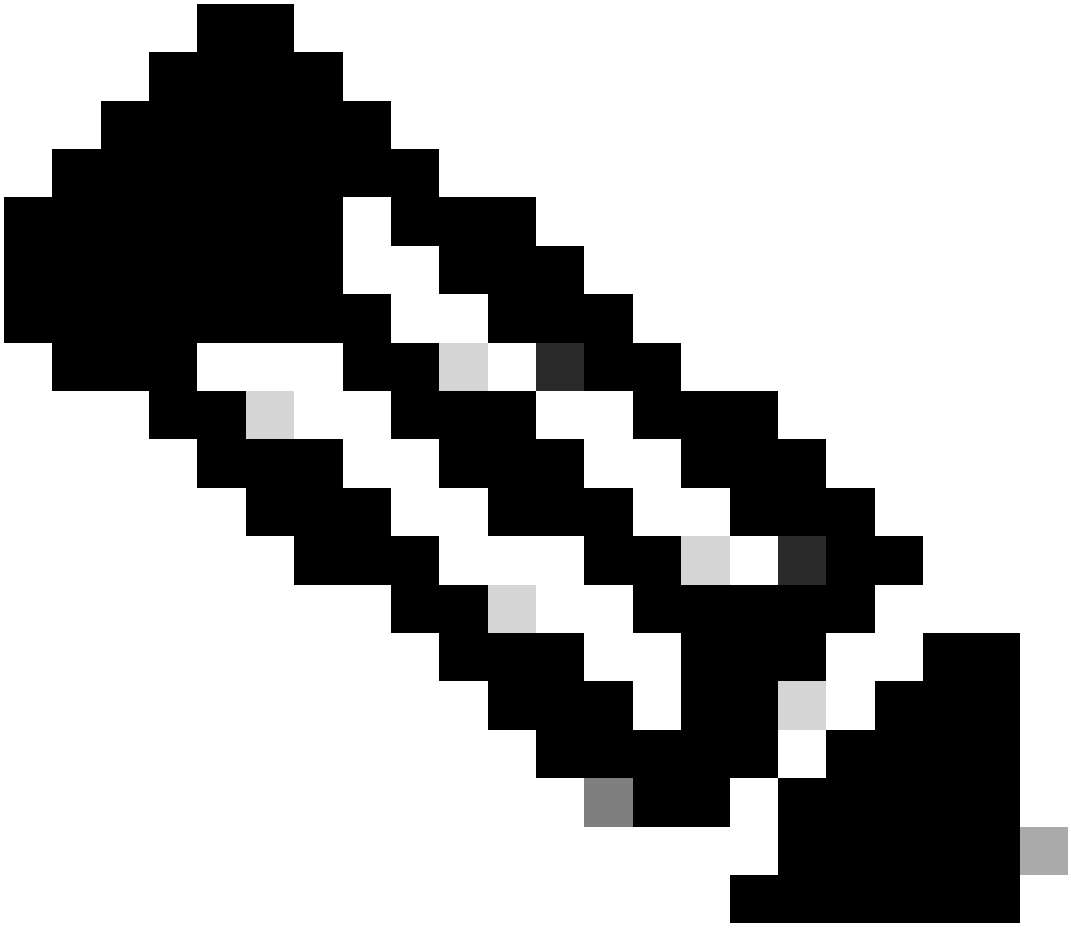
100 / 100
CVSS 3.1: 8.8

Heap buffer overflow in libwebp in Google Chrome prior to 116.0.5845.187 and libwebp 1.3.2 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: Critical)

Fixed By:

- USN-6368-1

Close



참고: 사용 가능한 수정 사항이 없는 경우 TAC에 문의하십시오.

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.