cojuscan

보안 진단 보고서

스캔 정보

진단일 2025. 7. 14.

스캔 엔진 Semgrep

버전 v1.4.0-beta

프로젝트 정보

경로

C:\Users\user\AppData\Local\Temp\cojuscan-iWMYiQ

번호	취약점	심각도	파일	라인
1	외부 리소스 무결성 검증 누락	Medium	index.html	8
2	커맨드 인젝션	High	install-semgrep.js	28
3	경로 탐색 (Path Traversal)	Medium	main.js	68
4	경로 탐색 (Path Traversal)	Medium	main.js	68
5	안전하지 않은 문자열 포맷팅	Low	main.js	81
6	경로 탐색 (Path Traversal)	Medium	main.js	332
7	경로 탐색 (Path Traversal)	Medium	main.js	353
8	경로 탐색 (Path Traversal)	Medium	main.js	353
9	안전하지 않은 문자열 포맷팅	Low	main.js	358
10	경로 탐색 (Path Traversal)	Medium	main.js	370
11	경로 탐색 (Path Traversal)	Medium	main.js	370
12	안전하지 않은 문자열 포맷팅	Low	main.js	559
13	안전하지 않은 문자열 포맷팅	Low	main.js	656
14	안전하지 않은 DOM 조작	High	renderer.js	319
15	안전하지 않은 DOM 조작	High	renderer.js	431
16	안전하지 않은 DOM 조작	High	renderer.js	438
17	안전하지 않은 DOM 조작	High	renderer.js	632
18	안전하지 않은 DOM 조작	High	renderer.js	788
19	안전하지 않은 DOM 조작	High	renderer.js	797

번호	취약점	심각도	파일	라인
20	안전하지 않은 DOM 조작	High	renderer.js	811
21	안전하지 않은 DOM 조작	High	renderer.js	828
22	안전하지 않은 DOM 조작	High	renderer.js	899
23	안전하지 않은 DOM 조작	High	renderer.js	1148
24	안전하지 않은 DOM 조작	High	renderer.js	1171
25	안전하지 않은 DOM 조작	High	renderer.js	1220
26	안전하지 않은 DOM 조작	High	renderer.js	1226
27	안전하지 않은 DOM 조작	High	renderer.js	1242
28	안전하지 않은 DOM 조작	High	renderer.js	1247
29	안전하지 않은 DOM 조작	High	renderer.js	1416
30	안전하지 않은 DOM 조작	High	renderer.js	1437
31	안전하지 않은 DOM 조작	High	renderer.js	1446
32	안전하지 않은 DOM 조작	High	renderer.js	1492
33	안전하지 않은 DOM 조작	High	renderer.js	1505
34	안전하지 않은 DOM 조작	High	renderer.js	1523
35	안전하지 않은 DOM 조작	High	renderer.js	1575
36	외부 리소스 무결성 검증 누락	Medium	report.html	7
37	안전하지 않은 DOM 조작	High	report.js	189
38	안전하지 않은 DOM 조작	High	report.js	226

총 발견 취약점 38

보안 점수 **0** **/ 100**

cojuscan

2025. 7. 14.

종합 진단 결과

진단 요약

이번 정밀 진단에서 총 38개의 잠재적 보안 취약점이 발견되었습니다. 이 중 0개는 무시 처리되었으며, 유효한 취약점은 **총 38개**입니다. 유효 취약점의 상세 분포는 **심각(High) 등급 25개, 중간(Medium) 등급 9개, 낮음(Low) 등급 4개**로 분석되었습니다.

주요 발견 취약점 (무시 항목 제외)

- **'안전하지 않은 DOM 조작'** 유형이 **24회** 발견되어 주요 위험 요소로 식별되었습니다.
- **'경로 탐색 (Path Traversal)'** 유형이 **7회** 발견되어 주요 위험 요소로 식별되었습니다.
- **'안전하지 않은 문자열 포맷팅'** 유형이 **4회** 발견되어 주요 위험 요소로 식별되었습니다.

상세 조치 권고

가장 시급하고 중요한 수정 사항은 다음과 같습니다.

> ***커맨드 인젝션:*** *외부 프로세스를 실행할 때 사용자 입력을 인자로 안전하게 전달하고, 고정된 명령어만 사용하도록 제한하세요. 불가피하게 `exec`를 사용해야 한다면, 사용자 입력을 쉘 메타문자로부터 엄격하게 이스케이프 처리해야 합니다.*

향후 계획

긴급 조치 이후, 근본적인 원인 해결을 위해 아키텍처 수준의 보안 설계를 재검토해야 합니다. 외부 보안 전문가의 컨설팅이나 모의 해킹을 통해 현재 인지하지 못한 다른 잠재적 위협이 있는지 확인하는 과정이 필수적입니다.

결론

즉각적인 조치가 필요한 보안 위협이 다수 발견되었습니다. '안전하지 않은 DOM 조작' 취약점 해결을 최우선 과제로 삼고, 전체 시스템에 대한 긴급 보안 점검을 수행할 것을 강력히 권고합니다.