주요 자바스크립트 기반 웹 UI·프레임워크 보안 취약점 대응 권고

[2025.12.9]

- 최근 자바스크립트 기반의 React(라이브러리)·Next.js(프레임워크)에서 심각한 보안 문제가 발견되어, 전 세계 많은 웹사이트가 영향을 받는 것으로 확인
- 취약점은 클라이언트↔서버 통신 과정에서 데이터 패킷의 무결성 검증이 정상적으로 이루어지지 않아 악의적인 코드를 인증 없이 원격으로 실행 가능

❶ 개 요

- 최근 전 세계 많은 웹사이트에서 사용 중인 자바스크립트 기반의 React(라이브러리)·Next.js(프레임워크)에서 영향을 받는 CVE-2025-55182·66478 취약점 발견
- 이에, 취약점 정보와 영향받는 제품 정보를 공유하오니 업데이트 조치 권고 바람

❷ 취약점 설명

- 클라이언트↔서버 통신 과정에서 데이터 패킷의 무결성 검증이 정상적으로 이루어지지 않아 공격자가 전달한 악의적인 코드를 인증 없이 원격 코드 실행(RCE) 가능
- Common Vulnerability Scoring System(CVSS) 위험도 점수 10.0 만점으로 평가 중

❸ 위험도

- 공격 코드(PoC)가 인터넷에 공개되어 취약한 서버 대상 대규모 스캐닝 및 침투 시도에 악용되어, 광범위한 피해로 이어질 가능성이 높은 것으로 평가

  - △암호화폐 채굴 △관리자 권한 탈취 △추가 악성코드 설치 등 2차 피해 정황도 확인

❹ 영향받는 제품 및 취약한 버전

취약점	영향받는 제품 및 패키지	취약한 버전	업데이트 권고 버전
CVE-2025-55182 CVE-2025-66478	react-server-dom-webpack	19.0	19.0.1
		19.1.0 ~ 19.1.1	19.1.2
		19.2.0	19.2.1
	react-server-dom-parcel	19.0	19.0.1
		19.1.0 ~ 19.1.1	19.1.2
		19.2.0	19.2.1
	react-server-dom-turbopack	19.0	19.0.1
		19.1.0 ~ 19.1.1	19.1.2
		19.2.0	19.2.1
	Next.js	15.0.x	15.0.5
		15.1.x	15.1.9
		15.2.x	15.2.6
		15.3.x	15.3.6
		15.4.x	15.4.8
		15.5.x	15.5.7
		16.0.x	16.0.7

❺ 설치된 라이브러리 및 프레임워크 확인 방법

- npm 또는 yarn 패키지 매니저를 사용하는 경우 아래 명령어를 통해 React 설치 여부 및 취약 버전 확인 가능

실행 명령어
npm list react react-server-dom-webpack react-server-dom-parcel react-server-dom-turbopack
yarn list —pattern "react$|react-server-dom-"

❻ 조치사항

- 각급 기관은 자체 확인 후 취약한 버전의 React가 설치된 경우 패치를 권고하며, 의심 악성코드 • 경유지 등 정보가 파악되면 'analysis@ncsc.go.kr'으로 신속 통보 바랍니다.