최신 웹 공격 관련 연구 결과 소개

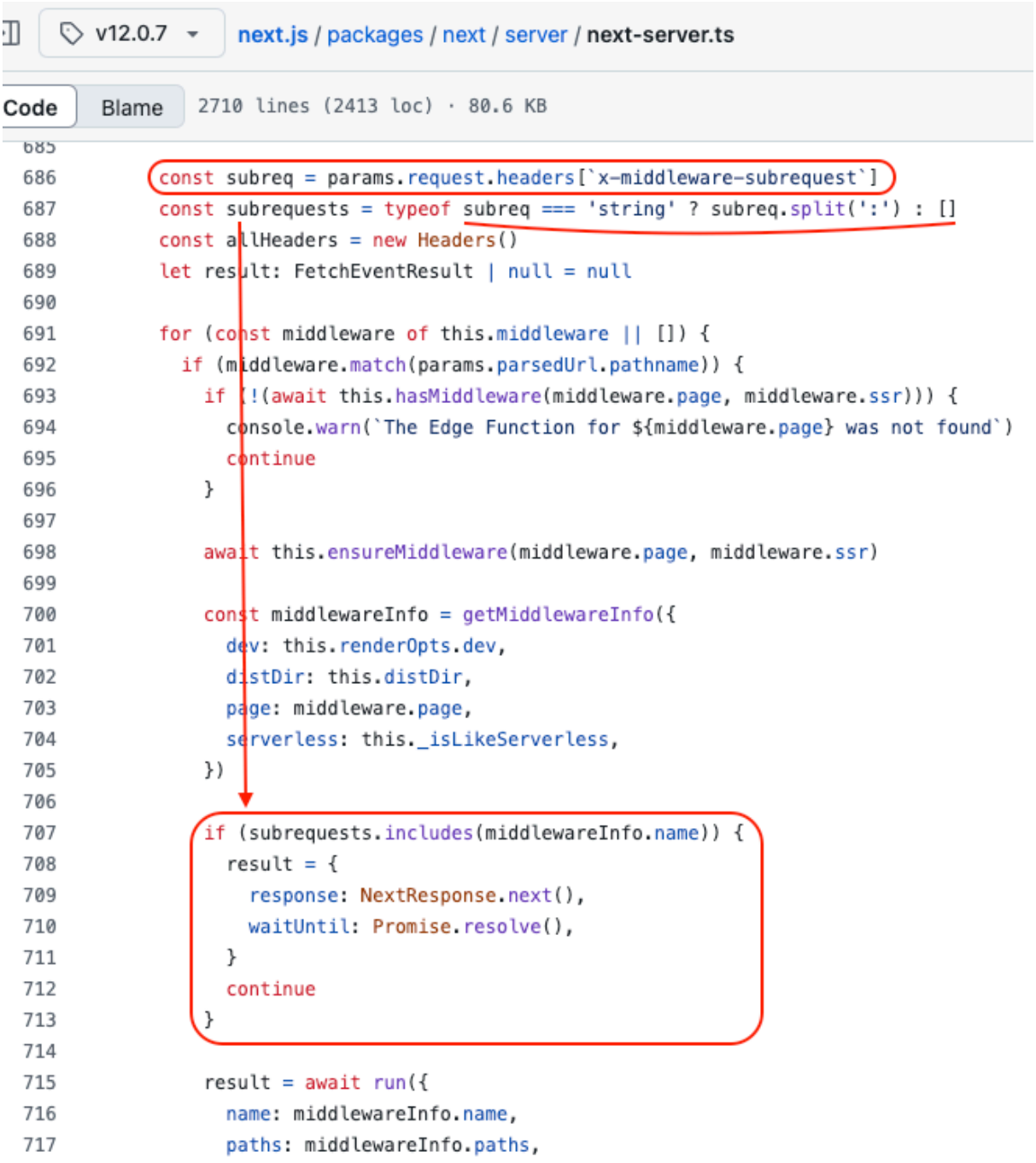
> [19반] 정민석_7000

CVE-2025-29927

내용 요약

Nextjs는 SSR 프레임워크로, 미들웨어를 통하여 API 등의 서비스를 관리합니다. 이때 Next.js and the corrupt middleware: the authorizing artifact 문서에는 인증되지 않은 사용자가 허용되지 않은 경로(ex. /dashboard/admin)로 접근할 수 있는 사례를 제시합니다.

취약점의 근본 원인 및 공격방법



위의 코드에서 `x-middleware-subrequest` 헤더가 `middlewareInfo.name`을 포함하면, 미들웨어가 적용되지 않습니다. 즉, 미들웨어의 인증 로직이 무력화되고, 공격자가 허용되지 않은 경로로 접근할 수 있게 됩니다.

하지만 `middlewareInfo.name`이 무엇인지 모른다면, 취약점의 심각도가 줄어들 것입니다. 하지만 해당 연구자는 미들웨어로 보호되고 있는 `/dashboard/panel/admin` 경로에 접근하기 위해서는, `middlewareInfo.name`이 `pages/_middleware`, `pages/dashboard/_middleware`, `pages/dashboard/panel/_middleware`를 포함하고 있음을 알아냈습니다. 즉, `x-middleware-subrequest` 헤더에 위의 3가지의 값 중 하나가 있다면 미들웨어를 우회할 수 있게 되며,

`middlewareInfo.name` 이 포함할 값을 찾는 것은 Nextjs 버전에 따라 로직이 다르지만, 손쉽게 파악할 수 있습니다.

공격의 파급도

Nextjs는 전세계적으로 널리 사용되고 있는 SSR 프레임워크이며 많은 서비스가 Nextjs로 운영됩니다. 더하여 해당 취약점은 버전에 따라 `x-middleware-subrequest` 에 담길 값을 도출하는 로직만 상이하였으며, 발견 당시 모든 버전에서 취약점이 작동하였습니다. 이를 통하여 권한 부여, CSP 우회 등이 가능해집니다. 이 취약점은 CVSS 9.1/10로 기록되었습니다.

방어 방법

Nextjs의 버전에 따라 취해야할 조치가 달라집니다.

- Next.js 15.x의 경우, 15.2.3 이상으로 업그레이드합니다.
- Next.js 14.x의 경우, 14.2.25 이상으로 업그레이드합니다.
- Next.js 11.1.4~13.5.6의 경우, x-middleware-subrequest가 포함된 요청을 도달하지 못하도록 해야합니다.

취약점 관련 자료를 수집한 방법

- 구글에 CVE-2025-29927를 검색하였습니다.
- https://projectdiscovery.io/blog/nextjs-middleware-authorization-bypass의 링크를 발견하였으며, 해당 페이지에서 최초 제보자의 블로그 글로 이동하였습니다.

[참고 문헌]

- https://zhero-web-sec.github.io/research-and-things/nextjs-and-the-corrupt-middleware
- https://projectdiscovery.io/blog/nextjs-middleware-authorization-bypass