Vercel 資安報告

> 主要是針對 Next.js 新架構 App Router 的 CVE 報告

React

DoS 攻擊

Denial of Service Vulnerability in React Server Components

High ⇒ React 在序列化 Server Components 的時候，可能被 Hacker Injection 自我引用的 SC 會導致 Infinite Loop

PS. 我在寫聚編系統時有遇到這個 Error. 編譯器會提醒開發者！

Next.js

Denial of Service with Server Components

High 同上，RSC 在序列化時的 DoS 風險

* Server Action 回傳的 JSON ⇒ 注意
* 限制 Payload 大小

PS. 我自己的解法是"明確"定義每個 Object 的 Type，且有意義的命名

Middleware / Proxy bypass in App Router applications via segment-prefetch routes

High ⇒ Next.js 在 <Link>、useRouter 這種室上路徑的 DOM，會執行 Prefetch Request，可能繞過 middleware.

PS. 外部反向代理（Cloudflare 等）可能要實"校驗" session、cookies，不要直接近入 Server

DoS

Denial of Service via connection exhaustion in applications using Cache Components

High ⇒ Hacker 發送特殊 Request 導致 App Router 中的 Cache 機制不釋放資源

PS. 升級 Next.js or 在 Nginx、Cloudflare 室連線超時切斷（還是 Cloudflare 已經 default 有這功能？I'm not sure）

Middleware / Proxy bypass through dynamic route parameter injection

High ⇒ 動態路由可能被 Injection 指令，導致繞過 Middleware

PS. WAF 要室防禦 Logic e.g. 特殊字元的路徑 Request 一律 400 Bad Request

SSRF

Server-side request forgery in applications using WebSocket upgrades

High ⇒ WebSoket 套件（這個 Package 具体用処為何自己上網查、說來話長）会被 Hacker 發送 Upgrade Request 導致深測內網

PS. 不要用 WebSoket or Server 的 FireBase 要室白名單

Middleware / Proxy bypass in Pages Router applications using i18n

High ⇒ i18n（多国語言套件）有問題，特殊語言的特殊字元会產生 Injection

PS. 我記得中心沒有 Page Router 的 Project 用到 i18n，但我前几天自己練習的 Project 有用到這套件，也有看到這 Bug

5/20/26

內容安全政策

XSS

Cross-site scripting in App Router applications using CSP nonces

Moderate ⇒ CSP 会被 Hacker 实入 script，导致 XSS

P.S. 升級 Next.js 是唯一解

XSS

Cross-site scripting in beforeInteractive scripts with untrusted input

Moderate ⇒ 在 Next.js 中可以使用此 attribute 来執行 script，在 Render 之前。(甚至可能更早)

可能被 Hacker 在安全防護前 XSS

P.S. 我有遇到這个錯誤過，解也很 easy，把 <script> 刪掉就好，or <script src="引"> 這樣不安"好"

DoS

Denial of Service in the Image Optimization API

Moderate ⇒ <Image> Tag 可能被 Hacker Prefetch 極端指令导致 DoS

指定 Image 優化 limit

P.S. 我前阵的 Practice Project 也有遇到，只要在 next.config 实就好了

Cache poisoning in React Server Component responses

Moderate ⇒ Hacker 发送特殊指令导致被 Next.js 誤認為 Server Components，导致污染 Cache

P.S. 一樣，升級 Next.js，官方修正了這个"誤認"

Cache poisoning via collisions in React Server Component cache-busting

Low

同上

⇒ 升級 Next.js！

Middleware / Proxy redirects can be cache-poisoned

Low

5/20/26