VIEŠAS PAVYZDYS / IŠGALVOTAS ATVEJIS

Saugumo patikros ataskaita

Aiškūs prioritetai vadovui. Konkretus taisymo planas komandai.

2026-10-13 LEIDIMAS / VERSIJA 1.0

Šis pavyzdys parodo, kaip atrodo išsami CodeArc saugumo patikros ataskaita. Aprašyta platforma ir įrodymai yra išgalvoti, tačiau CVE spragos ir jų taisymo būdai yra tikri.

Svarbiausia vadovui

Pirmiausia atnaujinkite du kritinius sistemos komponentus.

Šiame pavyzdyje per seną „Next.js middleware“ sluoksnį pašalinis gali atsidaryti vidinius puslapius neprisijungęs, o pažeidžiama „React Server Components“ versija leidžia serveryje paleisti svetimą kodą. Atnaujinkite abu paketus, tikrinkite teises prie duomenų ir pakartokite patikrą.

2 kritinės spragos	1 papildoma apsauga	3 radiniai iš viso

PAVYZDINĖ PLATFORMA

Klientų savitarna + administravimas

BŪSENA

Pavyzdys / išgalvoti duomenys

Kas pateikta ataskaitoje

02 Patikros apimtis, ribos ir radinių suvestinė

03 iki 05 Radiniai: poveikis verslui, įrodymai, taisymas ir patikra

06 Taisymo planas ir oficialūs šaltiniai

PAVYZDYS: Visos sistemos, radiniai ir įrodymai šiame dokumente yra išgalvoti.

VIEŠAS PAVYZDYS / IŠGALVOTAS ATVEJIS

Apimtis ir radinių suvestinė

Kiekviena patikra prasideda nuo aiškių ribų: kurias sistemas tikriname, kokią prieigą gavome ir ko sąmoningai nelietėme.

Pavyzdinės sistemos

Klientų savitarna	`portal.demo.example` Next.js aplikacija, maršrutų apsauga ir naršyklės antraštės
Administravimas	`admin.demo.example` React Server Components diegimas ir paketų sąrašas

Kas buvo tikrinta

Kliento pateiktas paketų sąrašas (lockfile), diegimo ir prieigos nustatymai bei HTTP atsakai. Paketų spragos vertinamos pagal tikrą įdiegtą versiją, o ne spėliojant iš išorės.

Kas nebuvo daroma

Nespėliojami slaptažodžiai, nesiunčiamos griaunančios užklausos, nekeliama dirbtinė apkrova, nelendama į vidinį tinklą ir nekopijuojami klientų duomenys.

Radinių suvestinė

ID	Radinys	Svarba	CVSS*	Psl.
CA-001	Vidiniai puslapiai saugomi tik pažeidžiamu Next.js middleware	**Kritinė**	9.1	03
CA-002	Neatnaujinti React Server Components leidžia vykdyti kodą	**Kritinė**	10.0	04
CA-003	Savitarnos puslapiuose nenustatyta CSP taisyklė	**Žema**	Nevertinta	05

* Oficialūs CVE kūrėjų CVSS v3.1 baziniai balai. Jie rodo pačios spragos rimtumą, o realus pavojus verslui priklauso nuo to, kaip sistema patalpinta, kaip tikrinamos teisės ir kokie duomenys joje laikomi.

Kuo tai skiriasi nuo nemokamos svetainės patikros

Nemokama viešo puslapio patikra parodo tik išorinius HTTPS ir naršyklės antraščių nustatymus. Serverio paketų spragoms, prieigos klaidoms ar verslo logikos skylėms rasti reikalingas sutartas auditas.

VIEŠAS PAVYZDYS / IŠGALVOTAS ATVEJIS

PAVYZDINIS RADINYS CA-001

Vidiniai puslapiai saugomi tik per middleware

KRITINĖ / TAISYTI NEDELSIANT

CVE-2025-29927 / CWE-285 / Next.js Middleware

9.1 / 10 Kūrėjų CVSS v3.1 bazinis balas

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

Ką tai reiškia verslui

Jei prisijungimas tikrinamas tik pažeidžiamame „Next.js middleware“ sluoksnyje, pašalinis gali šią patikrą apeiti ir atsidaryti prisijungusiems vartotojams skirtus puslapius. Ar bus matomi svetimi duomenys, priklauso nuo to, ar sesiją dar kartą tikrina pats duomenų užklausos kodas.

Pavyzdiniai įrodymai

Išgalvota ištrauka, parodanti, kaip ataskaitoje fiksuojama tiksli versija, maršrutas ir nustatymai.

```
target: https://portal.demo.example/account/invoices (fictional)
package: next@14.2.24 / self-hosted Node.js runtime
guard: src/middleware.ts -> matcher: ['/account/:path*']
handler: getInvoices() pasitiki middleware ir sesijos nebetikrina
status: pažeidžiama versija ir vieno sluoksnio apsauga pavyzdyje
```

Kaip sutvarkyti

Atnaujinkite „Next.js“ į pataisytą versiją pagal kūrėjų pranešimą. Niekada nepasikliaukite vien „middleware“ apsauga: vartotojo sesiją ir teises tikrinkite tiesiai ten, kur skaitomi duomenys ar vykdomi veiksmai.

Kaip įsitikinti, kad sutvarkyta

Patikrinkite įdiegtą „Next.js“ versiją serveryje. Pabandykite atidaryti vidinius adresus neprisijungę ir su skirtingomis rolėmis (įskaitant specialias vidines middleware antraštes). Sistema turi atmesti neleistinas užklausas.

Apimtis ir prielaidos

Pavyzdinis radinys paremtas išgalvotu savarankiško talpinimo atveju. Tikrame projekte poveikis priklauso nuo talpinimo būdo ir papildomų sesijos patikrų kode.

PAKARTOTINĖ PATIKRA: LAUKIAMA PATAISOS / PAVYZDYS

CVE-2025-29927 / Oficialus šaltinis CWE-285

VIEŠAS PAVYZDYS / IŠGALVOTAS ATVEJIS

PAVYZDINIS RADINYS CA-002

Serverio komponentai leidžia paleisti svetimą kodą

KRITINĖ / TAISYTI NEDELSIANT

CVE-2025-55182 / CWE-502 / React Server Components

10.0 / 10 Kūrėjų CVSS v3.1 bazinis balas

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Ką tai reiškia verslui

Pažeidžiamoje „React Server Components“ versijoje pašalinis asmuo be jokio prisijungimo gali paleisti savo kodą serveryje. Tai reiškia tiesioginę riziką serverio slaptažodžiams, duomenų bazei ir vidinėms sistemoms.

Pavyzdiniai įrodymai

Išgalvota ištrauka, parodanti, kaip ataskaitoje fiksuojama tiksli versija, maršrutas ir nustatymai.

```
target: https://admin.demo.example (fictional)
package: react-server-dom-webpack@19.1.1 (RSC enabled)
advisory: GHSA-fv66-9v8q-g76r / CVE-2025-55182
surface: viešas Flight adresas pasiekiamas be prisijungimo
status: pažeidžiama versija pavyzdiniame sąraše (ataka nevykdyta)
```

Kaip sutvarkyti

Nedelsiant atnaujinkite „react-server-dom-*“ paketus bei „Next.js“ į pataisytą versiją, iš naujo surinkite ir perleiskite visus serverio konteinerius. Laikini ugniasienės filtrai paketo atnaujinimo neatstoja.

Kaip įsitikinti, kad sutvarkyta

Patikrinkite įdiegtų paketų sąrašą ir veikiančius konteinerius visose aplinkose, kad neliktų senos versijos, ir įsitikinkite, jog įprasti serverio veiksmai (Server Actions) veikia sklandžiai.

Apimtis ir prielaidos

Nustatyta pagal pavyzdinį paketų sąrašą nevykdant realios atakos. Svetainėms, kuriose „React“ veikia tik naršyklėje be serverio komponentų, ši spraga negalioja.

PAKARTOTINĖ PATIKRA: LAUKIAMA PATAISOS / PAVYZDYS

CVE-2025-55182 / Oficialus šaltinis

CWE-502

VIEŠAS PAVYZDYS / IŠGALVOTAS ATVEJIS

PAVYZDINIS RADINYS CA-003

Savitarnos puslapiuose trūksta CSP taisyklės

ŽEMA / PAPILDOMA APSAUGA

CA-003 / Content-Security-Policy / naršyklės apsauga

Nustatymų pastaba: CVE ar CVSS balas nesuteikiamas.

Ką tai reiškia verslui

Nenustatyta „Content-Security-Policy“ (CSP) antraštė pati savaime nėra saugumo skylė, tačiau naršyklė neturi papildomo saugiklio, jei į puslapį kada nors patektų svetimas scenarijus (XSS).

Pavyzdiniai įrodymai

Išgalvota ištrauka, parodanti, kaip ataskaitoje fiksuojama tiksli versija, maršrutas ir nustatymai.

```
target: GET https://portal.demo.example/ HTTP/1.1 (fictional)
status: 200 OK / Content-Type: text/html; charset=utf-8
Strict-Transport-Security: max-age=63072000; includeSubDomains
X-Content-Type-Options: nosniff
Content-Security-Policy: <missing>
```

Kaip sutvarkyti

Aprašykite CSP taisyklę pagal tai, kokius scenarijus, stilius ir išorinius adresus savitarna iš tikrųjų naudoja. Pirmiausia įjunkite stebėjimo režimą (Report-Only), patikrinkite pranešimus ir tik tada įjunkite blokavimą.

Kaip įsitikinti, kad sutvarkyta

Patikrinkite pagrindinius puslapius bei peradresavimus ir įsitikinkite, kad prisijungimas, formos bei mokėjimai veikia be naršyklės klaidų.

Apimtis ir prielaidos

Pastebėta viename pavyzdiniame atsakyme. Taisyklę visada reikia pritaikyti prie konkrečios sistemos naudojamų mokėjimo ar kitų integracijų, o ne kopijuoti bendrą šabloną.

PAKARTOTINĖ PATIKRA: LAUKIAMA PATAISOS / PAVYZDYS

Content-Security-Policy / Oficialus šaltinis

VIEŠAS PAVYZDYS / IŠGALVOTAS ATVEJIS

Sutvarkyti, patikrinti, uždaryti

Kiekvienam radiniui paskirkite atsakingą inžinierių, o užduotį laikykite baigta tik tada, kai pataisa įdiegta ir patikrinta veikiančioje sistemoje.

01 **Patikrinti tikrą būklę**

Patikrinti įdiegtas paketų versijas, talpinimo būdą ir kur tiksliai tikrinamos vartotojo teisės (CA-001, CA-002).

02 **Atnaujinti ir įdiegti**

Atnaujinti „Next.js“ bei „React Server Components“ paketus, perrinkti konteinerius ir įdiegti visose aplinkose.

03 **Įjungti naršyklės apsaugą**

Paleisti CSP taisyklę stebėjimo režimu, patikrinti mokėjimus bei formas ir įjungti galutinį ribojimą (CA-003).

04 **Pakartoti patikrą**

Pereiti visus patikros žingsnius ir užfiksuoti įdiegtą versiją, datą bei galutinę būseną.

Kadangi tai išgalvotas ataskaitos pavyzdys, visi trys punktai čia palikti kaip atviros užduotys. Jokia reali sistema nebuvo tikrinta.

Oficialūs pranešimai ir standartai (tikrinta 2026-10-13)

Next.js saugumo pranešimas / CVE-2025-29927

React saugumo pranešimas / CVE-2025-55182

React tinklaraštis / RSC spragos aprašymas ir atnaujinimas

OWASP / Secure Headers Project

MDN / Content-Security-Policy dokumentacija

FIRST / CVSS v3.1 specifikacija

OWASP / Web Security Testing Guide

Norite tokios patikros savo sistemai?

Parašykite, ką norite patikrinti. Tikslią apimtį ir kainą sutarsime raštu prieš pradėdami darbus.

codearc.io/security info@codearc.io