Atsakingas informacijos apie pažeidžiamumą atskleidimas

auto sprendimai

Atsakingas informacijos apie pažeidžiamumą atskleidimas

Įmonių grupė „Eleving Group“ yra įsipareigojusi užtikrinti informacijos saugumą ir apsaugoti savo informacinius išteklius nuo kibernetinių grėsmių. Skatiname atsakingą informacijos apie saugumo spragas atskleidimą, kaip nustatyta šioje politikoje, ir kviečiame visus saugumo srities specialistus pranešti apie mūsų paslaugų bei išteklių saugumo spragas.

Taikymo sritis

Ši politika taikoma šiems domenams:

- *.autosprendimai.lt

Išimtis:

- Autodiscover.autosprendimai.lt
- autosprendimai.lt/.env, autosprendimai.lt/.aws/config ir autosprendimai.lt/.aws/credential (Naudojame netikrus failus, tikros informacijos čia nėra)

Užklausų skaičius neturi viršyti 3 užklausų per sekundę (apie 10 000 užklausų per valandą). Laukiame pranešimų apie saugumo spragas, tokias kaip scenarijų vykdymas keliose svetainėse (*Cross-Site Scripting*, XSS), SQL injekcijos, šifravimo klaidos, nuotolinis kodo vykdymas, autentifikavimo klaidos ir kt.

Šie testų tipai yra neleistini:

- Atsisakymo aptarnauti (DoS, DDoS) testai;
- Testai, atliekami brutaliai reikalaujant prisijungimo duomenų (*brute force credential compromise*);
- Socialinė inžinerija;
- Fizinės prieigos testavimas;
- Bet koks kitas netechninis pažeidžiamumo testavimas.

Teisinė informacija

Priimame pranešimus apie saugumo spragas pirmiau išvardyta apimtimi ir geranoriškai sutinkame nesiimti teisinių veiksmų prieš asmenis, kurie:

- laikėsi šios politikos reikalavimų ieškodami saugumo spragų;
- naudoja testavimo produktus ir paslaugas nepakenkdami mūsų sistemoms ir duomenims;
- užtikrina bet kokios apie saugumo spragas sužinotos informacijos konfidencialumą, kol nesibaigė abipusiu susitarimu nustatytas terminas.

Pasiliekame teisę priimti arba atmesti bet kokius pranešimus apie bet kokias saugumo spragas ir imtis veiksmų pagal savo vidaus taisykles bei tvarką.

Kaip pateikti pranešimą?

Jei manote, kad aptikote mūsų informacinių išteklių saugumo spragą, susisiekite su mumis el. pašto adresu security@eleving.com ir pateikite šią informaciją:

- Išsamų saugumo spragos aprašymą;
- Išsamią informaciją apie saugumo spragos išnaudojimo galimybes;
- Jei taikoma, pateikite nuorodą, ekrano nuotraukas arba bet kokią kitą informaciją, kuri padėtų mums nustatyti aptiktą saugumo spragą.

Ko tikimės iš Jūsų?

Atkreipkite dėmesį, kad atliekant pažeidžiamumo tyrimą labai svarbu laikytis šių taisyklių:

- įsipareigojate aptiktos saugumo spragos nenaudoti tam, kad pasiektumėte arba bandytumėte pasiekti Jums nepriklausančią informaciją (tik tam, kad įrodytumėte pažeidžiamumo egzistavimą);
- įsipareigojate aptiktos saugumo spragos nenaudoti tam, kad pašalintumėte arba pakeistumėte informaciją;
- įsipareigojate mums laiku pranešti apie aptiktą saugumo spragą ir leisti ją pašalinti, prieš pranešdami apie spragą visuomenei.

Ko galite tikėtis iš mūsų?

Finansinės kompensacijos nesiūlome, tačiau, kai saugumo spraga, apie kurią buvo pranešta, bus pašalinta, galėsime suteikti pagalbą ir informaciją, kad tyrėjas galėtų paskelbti savo publikaciją ir viešai nurodyti savo indėlį (jeigu dėl to bus pasiektas abipusis susitarimas).