Vastutustundlik turvalisuse haavatavusest teavitamine

easycar

Vastutustundlik turvalisuse haavatavusest teavitamine

Eleving Group on pühendunud andmete turvalisuse tagamisele ja oma inforessursside kaitsmisele küberohtude eest. Me toetame vastutustundlikku haavatavustest teavitamist ja nende avalikustamist vastavalt käesolevale poliitikale. Me julgustame kõiki turvalisuse kontrollijaid ja testijaid teavitama meid meie teenuste ja varade turvalisuse nõrkadest kohtadest.

Ulatus

Käesolev poliitika laieneb järgmistele domeenidele:

- *.easycar.ee

Välja arvatud:

- Autodiscover.easycar.ee
- easycar.ee/.env, easycar.ee/.aws/config ja easycar.ee/.aws/credential (oleme rakendanud peibutusfailide kasutamist, siin puudub kehtiv teave)

Päringute arv ei tohi ületada 3 päringut sekundis (umbes 10 000 päringut tunnis). Ootame aruandeid ja tagasisidet selliste haavatavuste kohta, mis puudutavad saidiülest skriptimist (XSS), SQL-i süste, krüpteerimis- ja autentimisvigu, koodi kaugkäivitust jne.

Järgmised testitüübid pole lubatud:

- Võrgu teenuse keelamise (DoS, DDoS) testid,
- *Brute-force* ehk ohustav jõuründe test,
- *Social engineering* ehk inimeste manipuleerimine saamaks andmetele ligipääsu,
- *Physical access testing* ehk reaalne katse füüsiliselt saada ligipääs seadmetele,
- Mis tahes muu mittetehniline haavatavuse test.

Õiguslik avalikustamine

Võtame haavatavuse aruandeid vastu ülaltoodud ulatuses ja nõustume mitte algatama heauskselt õiguslikke meetmeid isikute vastu, kes:

- On järginud meie poliitikat turvalisuse testimise ja uurimise ajal;
- On osalenud toodete ja teenuste testimises meie süsteeme ja andmeid kahjustamata;
- On hoidunud avastatud haavatavuse üksikasjade avalikustamisest enne vastastikku kokkulepitud aja möödumist.

Jätame endale õiguse vastu võtta või tagasi lükata mis tahes teateid mis tahes haavatavuste kohta ning tegutseda nende suhtes vastavalt meie sisereeglitele ja eeskirjadele.

Kuidas saate edastada meile infot avastatud haavatavuste kohta?

Kui te arvate end olevat avastanud meie teabeallikates mõne haavatavuse, võtke meiega ühendust aadressil security@eleving.com ja lisage sinna järgmine teave:

- Avastatud nõrga koha üksikasjalik kirjeldus;
- Üksikasjalik teave haavatavuse kasutamise kohta selle avastamisel;
- Võimalusel panna kaasa link, ekraanipildid või muu teave, mis aitab meil teie leitud haavatavust tuvastada.

Mida meie teilt ootame?

Pange tähele, et haavatavuse testimise ajal on üliloluline järgida allpool välja toodud reegleid.

- Te ei kasuta tuvastatud haavatavust teile mittekuuluvale teabele juurdepääsuks ega sellele juurde pääsemise proovimiseks (ainult haavatavuse tõendamiseks);
- Te ei kasuta tuvastatud haavatavust teabe eemaldamiseks või muutmiseks;
- Teavitate meid haavatavusest õigeaegselt ja lasete meil teatatud haavatavuse parandada enne selle avalikuks tegemist.

Mida meilt vastu oodata?

Rahalist hüvitist me ei paku, kuid haavatavuse lahenemisel võime aidata avastajal kirjutada valmis vastavasisuline artikkel ja tunnustada teda panuse andmise eest ka avalikult, kui selles on omavahel varasemalt kokku lepitud.