Տեղեկատվական անվտանգության խոցելիության բացահայտում

ավտոշուկա

«Eleving Group»-ը պարտավորվում է ապահովել իր տեղեկատվական ռեսուրսների անվտանգությունը և պաշտպանել այն կիբեր սպառնալիքներից:

Ընկերությունը խրախուսում է անվտանգության խոցելիության բացահայտումը և ողջունում է բոլոր այն անձանց, ովքեր կտեղեկացնեն մեր ծառայությունների և ռեսուրսների անվտանգության խոցելիության մասին:

Մենք ակնկալում ենք զեկույցներ՝ անվտանգության խոցելիության այնպիսի տեղեկությունների մասին, ինչպիսիք են՝ XSS, SQL ներմուծում, գաղտնագրման թերություններ, նույնականացման և այլ թերություններ:

1 Շրջանակ

- *.avto1.am

Բացառում:

- Autodiscover.avto1.am
- avto1.am/.env, avto1.am/.aws/config և avto1.am/.aws/credential (Մենք ստուգել ենք խաբեության ֆայլերի օգտագործումը, այստեղ հավաստի տեղեկություններ չկան:)

Հարցումների քանակը չպետք է գերազանցի 3 հարցում վայրկյանում (մոտավորապես 10 000 հարցում մեկ ժամում): Մենք ակնկալում ենք զեկույցներ այնպիսի խոցելիության մասին, ինչպիսիք են՝ Cross-Site Scripting (XSS), SQL ներարկումներ, գաղտնագրման թերություններ, կոդերի հեռավոր կատարում, իսկորոշման թերություններ և այլն:

Անվտանգության խոցելիության բացահայտման համար չի թույլատրվում կիրառել հետևյալ թեստերի տեսակները.

- Ծառայության բաշխված մերժում (DoS, DDoS),
- Տվյալների կոտրում,
- Սոցիալական ճարտարագիտություն
- Ֆիզիկական մուտքի փորձարկում
- Ոչ տեխնիկական խոցելիության ցանկացած այլ թեստավորում

Իրավական բացահայտում.

Մենք ընդունում ենք անվտանգության խոցելիության մասին հաշվետվությունները վերը թվարկված շրջանակների համար, և համաձայնում ենք, բարեխղճորեն իրավական գործողություններ չձեռնարկել այն անհատների դեմ, ովքեր՝

- Անվտանգության խոցելիության հետազոտության ժամանակ չեն խախտել սույն քաղաքականության դրույթները,
- Ապրանքների և ծառայությունների փորձարկմանը մասնակցելիս չեն վնասել մեր համակարգերը և տվյալները,
- Ձերծ են մնացել հայտնաբերված անվտանգության խոցելիության մանրամասները հանրությանը հայտնելուց՝ մինչև փոխադարձ համաձայնեցված ժամկետի ավարտը:

Մենք իրավունք ենք վերապահում ընդունել կամ մերժել խոցելիության մասին ցանկացած զեկույց և գործել ներքին կանոնների և ընթացակարգերի համաձայն:

Ինչպե՞ս կարող եք տեղեկացնել.

Եթե կարծում եք, որ մեր տեղեկատվական ռեսուրսներում խոցելիություն եք հայտնաբերել, խնդրում ենք կապ հաստատել մեզ հետ security@eleving.com հասցեով և ներառել հետևյալ տեղեկությունները.

- Խոցելիության մանրամասն նկարագրություն,
- Խոցելիության օգտագործման վերաբերյալ մանրամասն տեղեկատվություն,
- Հնարավորության դեպքում հղում, սքրինշոթ կամ ցանկացած այլ տեղեկատվություն, որը կարող է օգնել մեզ բացահայտել ձեր հայտնաբերած խոցելիությունը:

Ի՞նչ ակնկալիքներ ունենք ձեզանից.

Խնդրում ենք նկատի ունենալ, որ խոցելիության հետազոտության ժամանակ խիստ կարևոր է հետևել հետևյալ կանոններին.

- Չօգտագործել հայտնաբերված խոցելիությունը՝ ձեզ չպատկանող տեղեկատվություն մուտք գործելու կամ փորձելու համար (կիրառել միայն խոցելիության առկայությունը ապացուցելու համար),
- Չօգտագործել հայտնաբերված խոցելիությունը՝ տեղեկատվությունը հեռացնելու կամ փոփոխելու համար,
- Ժամանակին տեղեկացնել խոցելիության մասին և թույլ տալ շտկել այն՝ նախքան դրա հրապարակումը:

Ի՞նչ ակնկալել մեզանից.

Մենք ֆինանսական փոխհատուցում չենք առաջարկում, սակայն հաղորդված խոցելիությունը լուծվելուն պես, կարող ենք օգնություն և տեղեկատվություն տրամադրել Ձեր հրապարակման համար, եթե դրա վերաբերյալ առկա է եղել փոխադարձ համաձայնություն: