Odyssi - Data Exposure

25.06.2020

Guillem Lefait
guillem@hey.com
Schoelcher, Martinique

Vulnérabilité

Data exposure

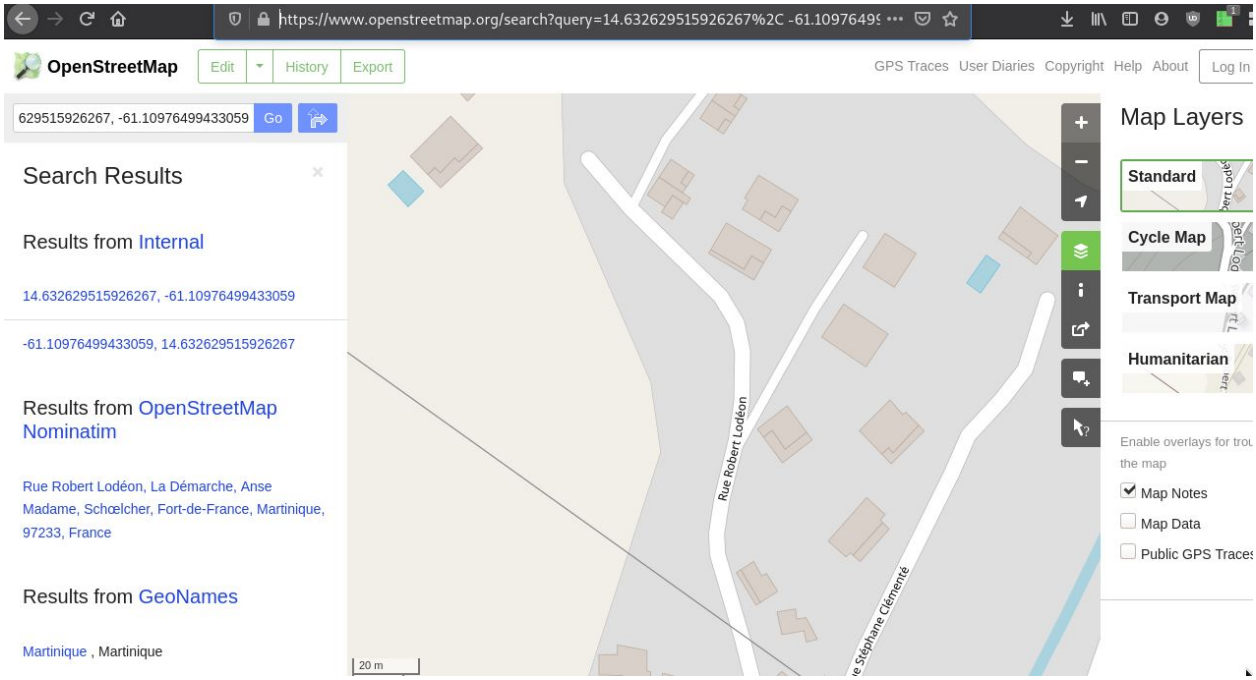
Il est possible de récupérer le ou les emplacements des alertes d'une personne, sans identification, en ayant connaissance de l'adresse email utilisé.

Le processus ne semble pas rate-limited ; et si c'était le cas, la protection ne serait pas idéale pour les attaques ciblés ou distribuées.

Exemple

```
$ curl -k 'https://www.odyssi.fr/coupure/alljsonAlerteDetails/guillem.lefait@gmail.com'

[{

    "title": "Alerte a supprimer",

    "description": "<strong>Alerte a supprimer<\/strong><br>\n
       <a href=\"https:\/\/www.odyssi.fr\/coupure\/4449\/alerteDestroy\">Supprimer<\/a>",

    "icon": "https:\/\/www.odyssi.fr\/theme\/images\/icons\/google-marker.png",

    "lat": "14.63298442532045",

    "lng": "-61.10989677687053"

}]
```

Les coordonnées peuvent être directement visualisée dans openstreetmap.



Ce qui correspond quasi parfaitement à la position de mon domicile.

Il y a donc un lien direct entre email et coordonnées GPS du domicile.

Impact

Pour les personnes vulnérables (ex: femmes victimes de violence, …), la possibilité de connaître la position de leurs alertes, et donc l'adresse de leur domicile, est bien sûr problématique.

De façon générale, le fait de pouvoir associer un email à une position géographique précise (différent d'une géolocalisation par IP qui est précise au maximum à 1 kilomètre autour du dernier point d'accès), est intrusif.

Pour une régie qui souhaite protéger les données personnelles de ses clients, c'est une mauvaise publicité.

Actions / Corrections

Data exposure

En dehors d'un système d'authentification qui réglerait le problème mais nécessiterait la maintenance de comptes, l'accès aux liens de gestion des alertes devraient se faire :

- soit après authentification via un lien temporaire envoyé sur l'adresse email
- soit directement dans un email envoyée à l'adresse configurée

Définition d'une politique de sécurité

Pour faciliter la remontée de ce genre de problème, je vous invite à définir une politique de divulgation responsable et d'implémenter la solution https://securitytxt.org/ .

Ces deux éléments permettent à la fois d'identifier rapidement qui contacter et de connaître le format et le contenu attendu.

Ce serait bien entendu très utile si d'autres problématiques venaient à être identifiées.

Remédiation

Sauf conditions particulières, cette remontée a vocation à être rendu publique au bout d'un délai raisonnable, fixé à 90 jours en suivant la politique standard google zero, c'est à dire à partir du 25 septembre 2020.

Au besoin, je me tiens disponible pour confirmer la résolution du problème.