Authentic 2 - Bug #60624

le token de changement d'email "contient de l'information"

13 janvier 2022 13:59 - Thomas Noël

Statut:	Nouveau	**Début:**	13 janvier 2022
Priorité:	Normal	**Echéance:**	
Assigné à:		**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Non	**Planning:**	Non

Description

De https://twitter.com/aeris22/status/1481311454586449924 (image jointe)

> Ah oui, ça rigole moyen sur les tailles de token de validation à la @CNIL
> Il y a une documentation quelque part sur le format du token, j'ai l'impression qu'il véhicule de l'information vu son format
> #ProtectionParLObscurité

De fait on utilise :

```
    token = signing.dumps(
        {
            'email': email,
            'user_pk': user.pk,
        }
    )
```

et apparemment c'est mal.

J'ai pas d'avis. Ça fait sortir des infos qui ne devraient pas ? Si vous voulez je demande des précision à https://twitter.com/aeris22/ (je sais même pas qui c'est, mais il a 6000 abonnés de bon niveau on dirait)

Il faudrait peut-être jouer en plus un coup de cryptage ?

Historique

#1 - 13 janvier 2022 14:19 - Benjamin Dauvergne

- Privée changé de Oui à Non

#2 - 13 janvier 2022 14:25 - Benjamin Dauvergne

On peut passer à un jeton opaque ou le chiffrer en plus de la signature HMAC qui est déjà ajoutée par Django, mais la présence de l'email est importante pour le throtting ou la possibilité d'avoir un bouton recommencer si le jeton est expiré (sans demander aux gens de retaper leur mail).

Au niveau diffusion de données; l'email ce n'est pas pertinent puisque c'est dans un mail qui déjà contient cette information en clair (pourquoi intercepter une requête HTTPs, c'est compliqué, quand on peut intercepter un mail, c'est plus simple). Pour le user_pk ça se discute, m'enfin faut casser une connexion TLS là aussi.

De toute façon si un truc demande d'avoir un compte en ligne relié à une donnée perso email ou téléphone ce ne sera jamais *tinfoilhat* proof, c'est juste pas possible.

#3 - 13 janvier 2022 15:12 - Aeris Imirhil

- Fichier email-verify-button.png ajouté

Bonjour ici :)
Je suis du coup l'auteur initial du tweet ci-dessus.

En l'état l'information véhiculée ne semble pas si critique que ça. On parle de l'email et de l'identifiant privée utilisateur.
L'email est en effet connu de celui qui clique sur le lien contenu dans l'email d'acceptation (surtout que les emails de départ et d'arrivée y sont rappelés), mais ce n'est pas forcément le cas des intermédiaires éventuellement présent sur la ligne (proxy d'entreprise, interception judiciaire, réseau Tor, etc, sachant que ces intermédiaires auraient de toute façon accès à plus derrière…).
On est d'accord que ça suppose des moyens importants ou qu'un attaquant serait certainement en mesure de collecter bien d'autres choses que ce lien.

Ça n'en reste pas moins une donnée à caractère personnel pour le coup, qui doit passer par une phase d'étude de minimisation et d'analyse de risque (surtout quand le client s'appelle la CNIL).
Ce jeton n'est même pas chiffré mais juste encodé puis signé cryptographiquement, je suppose qu'il doit être possible d'en décoder le contenu sans connaître la clef privée du serveur.

Un jeton banalisé aléatoire à faible durée de vie ne serait pas (ou en tout cas beaucoup moins et moins longtemps) une DCP et pourtant suffirait à valider une demande de changement d'adresse email.
Et sans le problème d'avoir à redemander l'email d'arrivée à l'utilisateur si la période de validation expire si celui-ci est stocké lors de la 1ère demande et qu'il suffit de recliquer sur un lien pour renvoyer un nouvel email de confirmation (cas classique qu'on retrouve chez Github et d'autres fournisseurs, cf copie d'écran ci-jointe).

#4 - 13 janvier 2022 15:52 - Benjamin Dauvergne

Aeris Imirhil a écrit :

> L'email est en effet connu de celui qui clique sur le lien contenu dans l'email d'acceptation (surtout que les emails de départ et d'arrivée y sont rappelés), mais ce n'est pas forcément le cas des intermédiaires éventuellement présent sur la ligne (proxy d'entreprise, interception judiciaire, réseau Tor, etc, sachant que ces intermédiaires auraient de toute façon accès à plus derrière…).

Ce sont ces intermédiaires qui seront responsables d'une fuite de DCP par manquement à leurs obligations donc; on ne peut pas assigner la responsabilité uniquement aux deux bouts de la chaîne. On rentre dans du juridique ici et pas du tout du technique, nous avons fait le best effort pour ne pas fuiter d'information, il n'y a effectivement pas de fuite ici, la fuite suppose une erreur entre l'envoi du mail et sa réception par l'usager sur sa boite mail et idem dans l'autre sens lors du clique (sachant que nous ne sommes pas hébergeur en plus). Si un utilisateur a une adresse Gmail ou chez un hébergeur français (interception judiciaire) ou n'importe quel autre hébergeur américain (allez disons 90% des usagers en étant pas généreux) tout effort ici est inutile si le danger est une interception judiciaire (mais je ne savais pas que le RGPD devait protéger les gens contre les interceptions judiciaires légales... qu'elles soient illégale au niveau du droit international sera encore une autre affaire). Idem si le poste client de la personne est vérolée (ou son environnement, proxy d'entreprise) nous n'y pouvons rien au niveau logiciel.

#5 - 13 janvier 2022 16:05 - Aeris Imirhil

Les intermédiaires seraient effectivement responsables, mais le responsable de traitement initial aussi.
Le RGPD n'interrompt justement plus la chaîne de responsabilité au premier responsable identifié mais la propage jusqu'au dernier responsable de traitement.

C'est comme ça qu'une entreprise s'est vue condamnée pour défaut de sécurisation suite à un délit commit par son salarié
Ou qu'un équivalent de la Banque de France espagnol s'est faite condamné pour défaut de base légal parce que quelqu'un avait usurpé de l'identité d'une personne et contractée un prêt

Dans votre cas, on pourrait certainement invoquer le manque de minimisation (5(c)) et de défaut de sécurisation (5(f)). En particulier ici la sécurité n'est justement pas suffisante pour se protéger des actes illicites, (« traitées de façon à garantir une sécurité appropriée des données à caractère personnel, *y compris la protection contre le traitement non autorisé ou illicite* », dans le texte du RGPD)

#6 - 13 janvier 2022 16:39 - Benjamin Dauvergne

Aeris Imirhil a écrit :

> Les intermédiaires seraient effectivement responsables, mais le responsable de traitement initial aussi.
> Le RGPD n'interrompt justement plus la chaîne de responsabilité au premier responsable identifié mais la propage jusqu'au dernier responsable de traitement.

Je veux bien un lien vers une analyse juridique sur ce point concernant le cas précis qui nous concerne. À défaut de pouvoir garantir la sécurité des mails de bout en bout nous devrions nous abstenir d'envoyer la moindre information personnelle par mail (c'est impossible autant ne pas envoyer de mail) ? Avez-vous l'avis d'un juriste compétent sur cette question ? Je ne peux pas garantir non plus la sécurité des SMS de bout en bout ou de quoi que ce soit de bout en bout, le mieux c'est de ne rien faire /s.

> C'est comme ça qu'une entreprise s'est vue condamnée pour défaut de sécurisation suite à un délit commit par son salarié

"vicariously liable" = "responsabilité du fait d'autrui", oui effectivement le droit finit toujours pas assigner une responsabilité à quelqu'un pour les dédommagements[1] sauf qu'il y a un lien de responsabilité via le salariat ici; aucun rapport avec ce que je dis, nous n'avons aucun partage de responsabilité avec les intermédiaires (et encore là c'est via une loi anglaise de 1998 aucun rapport avec le RGPD).

fn1: https://fiches-droit.com/responsabilite-du-fait-dautrui

> Ou qu'un équivalent de la Banque de France espagnol s'est faite condamné pour défaut de base légal parce que quelqu'un avait usurpé de l'identité d'une personne et contractée un prêt

Aucun rapport c'est un manquement au "due diligence" i.e. la banque n'a pas supprimé les données quand on lui a demandé.

> Dans votre cas, on pourrait certainement invoquer le manque de minimisation (5(c)) et de défaut de sécurisation (5(f)). En particulier ici la sécurité n'est justement pas suffisante pour se protéger des actes illicites, (« traitées de façon à garantir une sécurité appropriée des données à caractère personnel, *y compris la protection contre le traitement non autorisé ou illicite* », dans le texte du RGPD)

Pourquoi citez d'autres cas qui n'ont aucun rapport avant d'en arriver là ? Je suis pas certain du caractère bienveillant de ces remarques. Néanmoins les protections offertes par le RGPD ne sont pas absolues, elles nécessitent une évaluation du risque : https://gdprhub.eu/index.php?title=Article_32_GDPR le risque ici est minime, la fuite d'une adresse email ne peut mener à rien de grave et la fuite de la clé primaire de l'enregistrement dans la base n'est pas analysé/analysable (à vrai elle n'est pas utilisé autrement que par la brique de gestion d'identité, aucune corrélation n'est donc possible). La sécurisation en l'état me paraît suffisante.

#7 - 13 janvier 2022 17:04 - Aeris Imirhil

> Je veux bien un lien vers une analyse juridique sur ce point concernant le cas précis qui nous concerne.

Je vais essayer de vous retrouver ça. Dans ce cas précis ça serait la CNIL qui serait le responsable, pour le coup vous n'intervenez qu'en sous-traitant et (a priori) sans co-responsabilité de traitement.

> À défaut de pouvoir garantir la sécurité des mails de bout en bout nous devrions nous abstenir d'envoyer la moindre information personnelle par mail (c'est impossible autant ne pas envoyer de mail) ? Avez-vous l'avis d'un juriste compétent sur cette question ? Je ne peux pas garantir non plus la sécurité des SMS de bout en bout ou de quoi que ce soit de bout en bout, le mieux c'est de ne rien faire /s.

C'est ce type de problème qui effectivement conduit l'EBA à invalider les OTP par email ou par SMS, faute de pouvoir sécuriser correctement le vecteur de communication.

> Néanmoins les protections offertes par le RGPD ne sont pas absolues, elles nécessitent une évaluation du risque

Ça dépend. Il y a déjà eu 2 condamnations (Carrefour:https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042563756 et DSB:https://gdprhub.eu/index.php?title=DSB_(Austria)_-_2021-0.586.257_(D155.027)) qui ont montré que les protections doivent être absolues, quelque soit la réalité pratique et les probabilités de l'attaque en question.

Dans le cas précis ici du token d'acceptation, on est plus ou moins d'accord que le risque est assez/très limité.
Ne vous méprenez pas sur mes intentions, je me contenterai parfaitement de ce token même en l'état.
Mais c'est quand même une présence très étonnante vu le client en question, surtout sachant que la solution classique naïve d'un jeton aléatoire cochait toutes les cases.

#14 - 25 janvier 2024 21:50 - Benjamin Dauvergne

- Lié à Development #41792: Utiliser le système de token pour la création de compte ajouté

#15 - 25 janvier 2024 21:53 - Benjamin Dauvergne

- Lié à Development #41792: Utiliser le système de token pour la création de compte supprimé

#16 - 25 janvier 2024 21:53 - Benjamin Dauvergne

- Sujet changé de le token de changement de mot de passe "contient de l'information" à le token de changement d'email "contient de l'information"

Fichiers

Capture d'écran de 2022-01-13 13-53-02.png	73,7 ko	13 janvier 2022	Thomas Noël
email-verify-button.png	51,8 ko	13 janvier 2022	Aeris Imirhil