Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Direction interministérielle du numérique et du système d'information et de communication de l'État

Le 19/04/2019

NOTE AUX RÉDACTIONS
TCHAP : RÉSOLUTION LE 18 AVRIL D'UNE FAILLE DE SECURITÉ

Une faille de sécurité a été détectée et corrigée hier sur la version bêta de la messagerie instantanée de l'État Tchap sans compromission d'informations confidentielles. Retour sur l'incident.

Le 18 avril, un informaticien connu sur les réseaux sociaux sous le pseudonyme Elliot Alderson, signale via Twitter avoir détecté une faille sur Tchap avant son lancement officiel.

Dès signalement, l'équipe en charge de Tchap a pris contact avec lui et a aussitôt **désactivé** la fonctionnalité de création de compte touchée par cette faille. **En quelque heures, la faille a été corrigée et la fonctionnalité rétablie.**

La faille en question provenait d'un module open source Python utilisé par Tchap et servant au filtrage des adresses mails dans la création de compte (l'application étant réservée aux agents de l'État avec une adresse professionnelle).

En exploitant cette faille, Elliot Alderson a pu se créer un compte et rentrer dans l'application.

La DINSIC, qui opère le service, précise que :

- Elliot Alderson **est le seul à avoir exploité cette faille.**
- Il a **uniquement eu accès aux salons publics visibles** par tous les utilisateurs de la messagerie (par opposition aux salons privés, fermés et accessibles sur invitation).
- Il n'a eu accès à **aucune information confidentielle**, ni aux coordonnées des agents.
- Le compte d'Elliot Alderson a été **supprimé.**

La DINSIC rappelle que Tchap n'a pas vocation à traiter d'informations très sensibles : il s'agit d'une messagerie instantanée permettant aux agents de l'État d'échanger en temps réel sur les problématiques professionnelles du quotidien, en garantissant que les conversations restent hébergées sur le territoire national.

La version actuelle est une version bêta qui s'améliore en continu. La DINSIC se tient à l'écoute des experts de la société civile et prendra en compte tout retour qu'ils lui remonteraient en vue d'améliorer l'application.

Contact presse DINSIC
Rachel Wadoux 01.71.21.11.98 – 06.84.72.02.00
rachel.wadoux@modernisation.gouv.fr

Note technique d'incident

Déroulement :

- 10h20 : le compte twitter Elliot Alderson @fs0c131y indique avoir trouvé une faille de sécurité sur Tchap.
- Il contacte les services du Premier ministre pour les prévenir qu'il a réussi à s'inscrire dans Tchap, sans adresse mail professionnelle de l'État.
- 11h : la DINSIC qui opère l'application est alertée, les équipes techniques de Tchap prennent contact avec Elliot Alderson, qui leur décrit précisément son mode opératoire.
- 12h11 : après vérification, la DINSIC suspend la création de compte sur l'application. Le service continue à fonctionner normalement par ailleurs.
- 12h20 : le compte d'Elliot Alderson, seul à avoir utilisé cette faille, est supprimé.
- 12h30 : les équipes techniques engagent la production et le test d'un correctif.
- 15h : le correctif est déployé, le service d'inscription est réouvert. Fin de l'incident.

Origine :

Elliot Alderson @fs0c131y a révélé sur twitter l'origine de la faille : la vulnérabilité vient du module email.utils (librairie python), pour le traitement des adresses mails.

Contact presse DINSIC
Rachel Wadoux 01.71.21.11.98 – 06.84.72.02.00
rachel.wadoux@modernisation.gouv.fr