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

April 19, 2019

Note to news editors
Tchap: resolution of a security flaw on April 18th

A security flaw was detected and fixed yesterday on the beta version of Tchap, the French State's instant messaging application, before it caused any breach of confidential information, before the official launch of Tchap. Incident report.

On April 18th, a computer specialist known on social media under the pseudonym Elliot Alderson used Twitter to alert to the existence of a security flaw.

Immediately afterwards, the team in charge of Tchap made contact with him and **deactivated** the feature allowing account creation which was affected by this flaw. **Within a few hours, it was fixed and the feature restored.**

The flaw in question originated from a Python open source unit used by Tchap to filter the email addresses in the account creation process (indeed, the application is restricted to the State's agents via their professional email).

By exploiting this flaw, Elliot Alderson was able to create an account and enter the application.

The DINSIC, in charge of operating this service, indicates that:

- Elliot Alderson is **the only person to have exploited this flaw**.
- He **only gained access to public chat rooms that were open and visible** to all users of the messaging application (in contrast with private chat rooms which are restricted and accessible through invitation only).
- He **neither had access to confidential information**, nor to the agents' contact details.
- Elliot Alderson's account was **deleted.**

The DINSIC points out that Tchap is not intended to treat very sensitive informations: it's an instant messaging application allowing the State's agents to exchange in real-time on daily professional matters, all the while ensuring these conversations remain hosted on the national territory.

The actual beta version is continuously improving. The DINSIC welcomes, and will take into consideration, feedback from civil society experts aiming to improve the application.

Press contact DINSIC
Rachel Wadoux +33 (0)1.71.21.11.98 – +33 (0)6.84.72.02.00
rachel.wadoux@modernisation.gouv.fr

Technical incident report:

Sequence of events:

- 10:20 am: Elliot Alderson's Twitter account @fs0c131y indicates that he has found a security flaw on Tchap
- He makes contact with the French Prime Minister's services to inform them he has managed to create a Tchap account without a State professional email.
- 11 am: the DINSIC, which operates the application is notified, Tchap's technical teams make contact with Elliot Alderson who describes precisely his operating method.
- 12:11 pm: after verification, the DINSIC suspends the account creation feature of the application. Meanwhile, the service continues to function.
- 12:20 pm: Elliot Alderson's account, the only one to have exploited this breach, is deleted.
- 12:30 pm: the technical teams start developing and implementing a correction.
- 3 pm: the correction is deployed, the subscription feature is restored. End of incident.

Origin:

Elliot Alderson @fs0c131y has revealed the origin of the breach on Twitter: the vulnerability originates from the email.utils (Python library) unit, used to process email addresses.

Press contact DINSIC
Rachel Wadoux +33 (0)1.71.21.11.98 – +33 (0)6.84.72.02.00
rachel.wadoux@modernisation.gouv.fr