AIRNITE

ZERO DAY

NUMÉRO 06/2026 · SÉCURITÉ INFORMATIQUE

La clé dans le widget de chat : comment des jetons OAuth volés ont ouvert des données Salesforce

En août 2025, des attaquants ont utilisé des jetons d'accès volés d'une intégration de chat pour interroger les instances Salesforce de nombreuses entreprises – sans faille dans Salesforce lui-même. Ce qui s'est passé et comment sécuriser vos intégrations.

Publié le: 21 novembre 2026 Temps de lecture: 6 min Auteur: Rédaction Airnite

// LA SITUATION EN CHIFFRES

08–18/08/2025
période des requêtes
au moins ; Google Threat Intelligence Group

0
faille dans Salesforce
accès via des jetons volés d'une application tierce (GTIG)

AKIA…
clés AWS recherchées
ainsi que mots de passe et jetons Snowflake dans les données (GTIG)

20/08/2025
tous les jetons Drift révoqués
Salesloft avec Salesforce, selon GTIG

De nombreuses entreprises connectent de petits outils à leur CRM : widgets de chat, outils commerciaux, automatisations. Chaque intégration reçoit une clé numérique, un jeton OAuth, qui lui donne un accès durable aux données. En août 2025, on a vu ce qui se passe quand ces clés tombent entre de mauvaises mains.

// Que s'est-il passé ?

Selon le Google Threat Intelligence Group (GTIG), un groupe désigné **UNC6395** a utilisé, au moins **du 8 au 18 août 2025**, des jetons OAuth volés de l'application tierce **Salesloft Drift** pour accéder aux instances Salesforce de clients. Aucune faille de Salesforce n'a été nécessaire : les attaquants se connectaient avec les droits de l'intégration.

Le 20 août 2025, selon GTIG, Salesloft et Salesforce ont révoqué tous les jetons d'accès et de rafraîchissement actifs de l'application Drift ; Salesforce a retiré provisoirement Drift de son AppExchange. Une mise à jour du 28 août 2025 a élargi le périmètre : les jetons de l'intégration « Drift Email » étaient aussi compromis, et les attaquants s'en sont servis le 9 août pour accéder aux e-mails d'un très petit nombre de comptes Google Workspace. Google souligne que ni Workspace ni Alphabet n'ont été compromis.

// Comment fonctionne l'attaque ?

Selon GTIG, les attaquants ont interrogé systématiquement des objets Salesforce : comptes, opportunités, utilisateurs et tickets de support. Leur véritable cible n'était toutefois pas les données clients elles-mêmes, mais les **identifiants** qu'elles contenaient. GTIG cite des clés d'accès AWS (reconnaissables au préfixe « AKIA »), des mots de passe et des jetons pour la plateforme de données Snowflake. Copier de tels secrets dans des tickets ou des notes transforme le CRM en coffre au trésor.

Selon GTIG, les attaquants ont cherché à masquer leurs traces en supprimant leurs tâches de requête. Les journaux sont toutefois restés intacts, ce qui a permis de retracer l'attaque. GTIG cite comme indicateurs certains user-agents et adresses IP, dont des nœuds de sortie Tor.

// Qui est concerné ?

Selon GTIG, les clients ayant relié Drift à Salesforce étaient touchés ; selon Salesloft, les clients sans cette intégration ne l'étaient pas. Mais le schéma vaut pour toute entreprise qui connecte des applications tierces à ses systèmes centraux. Chaque intégration est un accès permanent, souvent moins surveillé qu'un compte humain – et sa clé se trouve chez le fournisseur, pas chez vous.

La situation devient critique quand des secrets sont stockés dans le CRM lui-même. Une fuite chez le fournisseur mène alors directement à votre cloud ou à vos bases de données.

// Que faire maintenant ?

GTIG recommande d'examiner toutes les intégrations tierces, de révoquer et renouveler les identifiants et de rechercher dans ses propres données les secrets stockés, par exemple « AKIA », « password » ou « secret ». S'y ajoutent l'analyse des journaux, la limitation des droits des applications connectées, des restrictions IP et des sessions courtes. La check-list ci-dessous résume les étapes.

// Comment Airnite vous aide-t-il ?

En **conseil**, Airnite établit avec vous l'inventaire de toutes les intégrations et de leurs droits, et fait le ménage. Lors d'un **test d'intrusion**, nous vérifions quels secrets traînent dans vos systèmes et jusqu'où un attaquant irait avec un jeton volé. Lorsque nous construisons pour vous des **workflows IA et automatisations**, nous appliquons dès le départ le moindre privilège, des jetons de courte durée et la journalisation.

> Remarque : les informations reposent principalement sur l'analyse du Google Threat Intelligence Group. Nous n'avons pas pu consulter directement les pages de Salesloft et de Salesforce consacrées à l'incident. État de la recherche : 21 novembre 2026.

Check-list : ce qu'il faut faire maintenant

[+] Lister toutes les applications connectées et intégrations OAuth du CRM, de la messagerie et du cloud, et supprimer celles qui sont inutiles.

[+] Limiter les droits des intégrations au strict nécessaire, définir des restrictions IP et des délais de session.

[+] Après un incident chez un fournisseur, révoquer et réémettre tous les jetons et identifiants associés.

[+] Rechercher les secrets stockés dans les fiches, tickets et notes (par ex. « AKIA », « password », « secret »), puis les supprimer et les renouveler.

[+] Activer la journalisation des requêtes API et surveiller les requêtes massives inhabituelles et les user-agents inconnus.

[+] Demander aux équipes de ne jamais écrire de mots de passe ou de clés dans des tickets ou des champs du CRM.

Comment Airnite vous aide

- Conseil – Un regard extérieur sur vos projets.
- Tests d'intrusion et sécurité – Attaques contrôlées avec rapport clair et plan d'action.
- Workflows IA et automatisation – Une IA qui travaille vraiment, avec règles et contrôle.

Quelles applications accèdent à vos données clients ?

Airnite inventorie les applications et intégrations connectées à vos systèmes CRM, marketing et cloud, vérifie les droits et la durée de vie des jetons et recherche les identifiants stockés dans des tickets, notes ou fiches. Vous recevez une liste de nettoyage priorisée.

Demander un premier échange · Écrire un e-mail · Par WhatsApp

Contact

Des questions sur cet article ? Écrivez-nous sur WhatsApp : +49 174 6834842

Lire en ligne: https://airnite.de/fr/magazine/salesloft-drift-vol-jetons-oauth/

Sources

Chaque fait de cet article repose sur les sources ci-dessous. Les sources primaires sont signalées.

1. **Google Threat Intelligence Group · Widespread Data Theft Targets Salesforce Instances via Salesloft Drift** · 26/08/2025, mise à jour 28/08/2025 · SOURCE PRIMAIRE
   Source primaire : acteur UNC6395, période, méthode, données recherchées, révocation des jetons, extension à Drift Email, recommandations
   https://cloud.google.com/blog/topics/threat-intelligence/data-theft-salesforce-instances-via-salesloft-drift
2. **The Register · Salesforce data missing? It might be due to Salesloft breach, Google says** · 27/08/2025
   Presse spécialisée : contexte
   https://www.theregister.com/2025/08/27/salesforce_salesloft_breach/
3. **heise online · Salesloft Drift: Login token misused for data theft** · 2025
   Presse spécialisée : compte rendu de l'incident
   https://heise.de/-10627153

Information éditoriale générale, sans conseil juridique ni examen individuel de vos systèmes. État : date de publication.

Airnite GmbH · Am Waldbach 7 · 77654 Offenburg · airnite.de