AIRNITE

ZERO DAY

ISSUE 06/2026 · IT SECURITY

The key in the chat widget: how stolen OAuth tokens opened up Salesforce data

In August 2025, attackers used stolen access tokens from a chat integration to query data from many companies' Salesforce instances – without any flaw in Salesforce itself. What happened and how to secure your integrations.

Published: 21 November 2026 Reading time: 6 min Author: Airnite editorial team

SOFTWARE. SECURITY. CODE.

// THE SITUATION IN NUMBERS

8–18 Aug 2025
period of data queries
at least; Google Threat Intelligence Group

0
flaws in Salesforce itself
access via stolen tokens of a third-party app (GTIG)

AKIA…
AWS keys hunted for
plus passwords and Snowflake tokens in the data (GTIG)

20 Aug 2025
all Drift tokens revoked
Salesloft with Salesforce, according to GTIG

Many companies connect small helpers to their CRM: chat widgets, sales tools, automations. Each of these integrations is given a digital key, an OAuth token, that lets it access data permanently. In August 2025, it became clear what happens when such keys fall into the wrong hands.

// What happened?

According to the Google Threat Intelligence Group (GTIG), a group designated **UNC6395** used stolen OAuth tokens from the third-party app **Salesloft Drift** from at least **8 to 18 August 2025** to access customers' Salesforce instances. No vulnerability in Salesforce itself was needed: the attackers logged in with the integration's permissions.

On 20 August 2025, according to GTIG, Salesloft and Salesforce revoked all active access and refresh tokens for the Drift application; Salesforce temporarily removed Drift from its AppExchange. An update on 28 August 2025 widened the scope: tokens for the "Drift Email" integration had also been compromised, and through them the attackers accessed emails from a very small number of Google Workspace accounts on 9 August. Google stresses that Workspace and Alphabet themselves were not compromised.

// How does the attack work?

According to GTIG, the attackers used the tokens to systematically query Salesforce objects: accounts, opportunities, users and support cases. Their real target, however, was not the customer data itself but the **credentials** stored in it. GTIG names AWS access keys (recognisable by the "AKIA" prefix), passwords and tokens for the Snowflake data platform. Anyone who copies such secrets into support cases or notes turns the CRM into a treasure chest.

According to GTIG, the attackers showed awareness of operational security: they deleted their query jobs. The logs, however, remained intact – which is why the attack could be traced. GTIG lists certain user-agent strings and IP addresses, including Tor exit nodes, among the indicators.

// Who is affected?

According to GTIG, customers who had connected Drift to Salesforce were affected; according to Salesloft, customers without this integration were not. But the pattern applies to every company that connects third-party apps to central systems. Each integration is a permanent access path that is often monitored less closely than a human account – and its key sits with the vendor, not with you.

It becomes particularly critical when secrets are stored in the CRM itself. A data leak at the vendor then leads straight into your cloud or your databases.

// What should you do now?

GTIG recommends reviewing all third-party integrations, revoking and rotating credentials and searching your own records for stored secrets, for example for “AKIA”, “password” or “secret”. Add log analysis, restricted permissions for connected apps, IP restrictions and short session times. The checklist below sums up the steps.

// How does Airnite help?

In **consulting**, Airnite works with you to create an overview of all integrations and their permissions, and cleans up. In a **penetration test**, we check which secrets are lying around in your systems and how far an attacker would get with a stolen token. When we build **AI workflows and automations** for you, we use minimal permissions, short token lifetimes and logging from the start.

> Note: the information is based mainly on the Google Threat Intelligence Group's analysis. We were unable to view Salesloft's and Salesforce's own incident pages directly. Research status: 21 November 2026.

Checklist: what to do now

[+] List all connected apps and OAuth integrations in CRM, email and cloud, and remove those you do not need.

[+] Limit integration permissions to the minimum, and set IP restrictions and session timeouts.

[+] After an incident at a vendor, revoke and reissue all related tokens and credentials.

[+] Search records, tickets and notes for stored secrets (e.g. “AKIA”, “password”, “secret”), then remove and rotate them.

[+] Enable logging of API queries and check for unusual bulk queries and unfamiliar user agents.

[+] Instruct staff never to write passwords or keys into support cases or CRM fields.

How Airnite helps

- Consulting – An outside view of your plans and projects.
- Penetration Testing & Security – Controlled attacks with a clear report and action plan.
- AI Workflows & Automation – AI that does real work, with rules and control.

Which apps have access to your customer data?

Airnite inventories the connected apps and integrations of your CRM, marketing and cloud systems, reviews permissions and token lifetimes and searches for credentials sitting in tickets, notes or records. You get a prioritised clean-up list.

Request an initial call · Send an email · Via WhatsApp

Contact

Questions about this article? Message us on WhatsApp: +49 174 6834842

Read online: https://airnite.de/en/magazine/salesloft-drift-oauth-token-theft/

Sources

Every fact in this article is based on the sources below. Primary sources are marked.

1. **Google Threat Intelligence Group · Widespread Data Theft Targets Salesforce Instances via Salesloft Drift** · 26 Aug 2025, updated 28 Aug 2025 · PRIMARY SOURCE
   Primary source: actor UNC6395, time window, method, data sought, token revocation, extension to Drift Email, recommendations
   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 Aug 2025
   Trade press: context
   https://www.theregister.com/2025/08/27/salesforce_salesloft_breach/
3. **heise online · Salesloft Drift: Login token misused for data theft** · 2025
   Trade press: report on the incident
   https://heise.de/-10627153

General editorial information, not legal advice and not an assessment of your individual systems. Status: date of publication.

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