AIRNITE

ZERO DAY

NÚMERO 06/2026 · SEGURIDAD INFORMÁTICA

La llave en el widget de chat: cómo unos tokens OAuth robados abrieron datos de Salesforce

En agosto de 2025, unos atacantes usaron tokens de acceso robados de una integración de chat para consultar datos de instancias de Salesforce de muchas empresas, sin ningún fallo en el propio Salesforce. Qué pasó y cómo proteger sus integraciones.

Publicado: 21 de noviembre de 2026 Tiempo de lectura: 6 min Autor: Redacción de Airnite

// LA SITUACIÓN EN CIFRAS

08–18/08/2025
periodo de las consultas
como mínimo; Google Threat Intelligence Group

0
fallos en el propio Salesforce
acceso mediante tokens robados de una app de terceros (GTIG)

AKIA…
claves de AWS buscadas
además de contraseñas y tokens de Snowflake en los datos (GTIG)

20/08/2025
todos los tokens de Drift revocados
Salesloft con Salesforce, según GTIG

Muchas empresas conectan pequeñas herramientas a su CRM: widgets de chat, herramientas de ventas, automatizaciones. Cada integración recibe una llave digital, un token OAuth, que le da acceso permanente a los datos. En agosto de 2025 se vio lo que pasa cuando esas llaves caen en malas manos.

// ¿Qué ha pasado?

Según el Google Threat Intelligence Group (GTIG), un grupo denominado **UNC6395** usó, al menos **del 8 al 18 de agosto de 2025**, tokens OAuth robados de la app de terceros **Salesloft Drift** para acceder a instancias de Salesforce de clientes. No hizo falta ningún fallo de Salesforce: los atacantes entraban con los permisos de la integración.

El 20 de agosto de 2025, según GTIG, Salesloft y Salesforce revocaron todos los tokens de acceso y de actualización activos de la aplicación Drift; Salesforce retiró Drift provisionalmente de su AppExchange. Una actualización del 28 de agosto de 2025 amplió el alcance: también se habían comprometido tokens de la integración «Drift Email», y con ellos los atacantes accedieron el 9 de agosto al correo de un número muy reducido de cuentas de Google Workspace. Google subraya que ni Workspace ni Alphabet fueron comprometidos.

// ¿Cómo funciona el ataque?

Según GTIG, con los tokens los atacantes consultaron de forma sistemática objetos de Salesforce: cuentas, oportunidades, usuarios y casos de soporte. Pero su verdadero objetivo no eran los datos de clientes en sí, sino las **credenciales** guardadas en ellos. GTIG menciona claves de acceso de AWS (reconocibles por el prefijo «AKIA»), contraseñas y tokens de la plataforma de datos Snowflake. Quien copia esos secretos en casos de soporte o notas convierte el CRM en un cofre del tesoro.

Según GTIG, los atacantes intentaron ocultar su rastro borrando sus tareas de consulta. Sin embargo, los registros se conservaron, y por eso pudo reconstruirse el ataque. GTIG cita como indicadores determinados user agents y direcciones IP, entre ellas nodos de salida de Tor.

// ¿A quién afecta?

Según GTIG, estaban afectados los clientes que habían conectado Drift con Salesforce; según Salesloft, los clientes sin esa integración no lo estaban. Pero el patrón vale para cualquier empresa que conecte apps de terceros a sus sistemas centrales. Cada integración es un acceso permanente, a menudo menos vigilado que una cuenta humana, y su llave está en manos del proveedor, no en las suyas.

La situación se vuelve crítica cuando en el propio CRM hay secretos guardados. Una fuga en el proveedor lleva entonces directamente a su nube o a sus bases de datos.

// ¿Qué hay que hacer ahora?

GTIG recomienda revisar todas las integraciones de terceros, revocar y renovar las credenciales y buscar en los propios registros secretos guardados, por ejemplo «AKIA», «password» o «secret». A ello se suman el análisis de registros, permisos limitados para las apps conectadas, restricciones de IP y sesiones cortas. La lista de control de abajo resume los pasos.

// ¿Cómo ayuda Airnite?

En la **consultoría**, Airnite elabora con usted un inventario de todas las integraciones y sus permisos, y pone orden. En una **prueba de penetración** comprobamos qué secretos hay sueltos en sus sistemas y hasta dónde llegaría un atacante con un token robado. Cuando creamos para usted **flujos de IA y automatizaciones**, aplicamos desde el principio permisos mínimos, tokens de corta duración y registro de actividad.

> Nota: la información se basa sobre todo en el análisis del Google Threat Intelligence Group. No pudimos consultar directamente las páginas de Salesloft y Salesforce sobre el incidente. Estado de la investigación: 21 de noviembre de 2026.

Lista de control: qué hacer ahora

[+] Enumere todas las apps conectadas e integraciones OAuth del CRM, el correo y la nube, y elimine las que no necesite.

[+] Limite los permisos de las integraciones a lo imprescindible y configure restricciones de IP y tiempos de sesión.

[+] Tras un incidente en un proveedor, revoque y vuelva a emitir todos los tokens y credenciales relacionados.

[+] Busque secretos guardados en registros, tickets y notas (p. ej. «AKIA», «password», «secret»), elimínelos y renuévelos.

[+] Active el registro de las consultas a la API y vigile consultas masivas inusuales y user agents desconocidos.

[+] Indique a la plantilla que nunca escriba contraseñas ni claves en casos de soporte o campos del CRM.

Cómo ayuda Airnite

- Consultoría – Una mirada externa sobre sus planes y proyectos.
- Pruebas de penetración y seguridad – Ataques controlados con un informe claro y un plan de medidas.

- Flujos de trabajo con IA y automatización – IA que hace trabajo real, con reglas y control.

¿Qué apps tienen acceso a los datos de sus clientes?

Airnite inventaría las apps e integraciones conectadas a sus sistemas de CRM, marketing y nube, revisa permisos y vida útil de los tokens y busca credenciales guardadas en tickets, notas o registros. Recibe una lista de limpieza priorizada.

Solicitar una primera conversación · Escribir un correo · Por WhatsApp

Contacto

¿Preguntas sobre este artículo? Escríbanos por WhatsApp: +49 174 6834842

Leer en línea: https://airnite.de/es/revista/salesloft-drift-robo-tokens-oauth/

Fuentes

Cada dato de este artículo se basa en las fuentes indicadas a continuación. Las fuentes primarias están señaladas.

1. **Google Threat Intelligence Group · Widespread Data Theft Targets Salesforce Instances via Salesloft Drift** · 26/08/2025, actualizado el 28/08/2025 · FUENTE PRIMARIA
   Fuente primaria: actor UNC6395, periodo, método, datos buscados, revocación de tokens, ampliación a Drift Email, recomendaciones
   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
   Prensa especializada: contexto
   https://www.theregister.com/2025/08/27/salesforce_salesloft_breach/
3. **heise online · Salesloft Drift: Login token misused for data theft** · 2025
   Prensa especializada: información sobre el incidente
   https://heise.de/-10627153

Información editorial general, no constituye asesoramiento jurídico ni una evaluación de sus sistemas concretos. Vigencia: fecha de publicación.

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