Lowenstein Sandler

Client Alert

Data, Privacy & Cybersecurity

August 29, 2025

UPDATE: Organizations Using the Salesloft Drift AI Chat Agent Must Check It for Compromise

By Amy S. Mushahwar, Kathleen A. McGee, and Cairon S. Overton

Security Orgs Now Publicizing Impact Beyond Salesloft-Salesforce Integrations

Yesterday, Mandiant issued an update to its previous Salesloft Drift advisory. Therein, Mandiant discussed that Salesloft issued a security notification on Aug. 26 regarding its Drift application. At that time, it appeared to be a broad opportunistic attack on Salesloft Drift instances integrated with Salesforce tenants. It appears that this broadscale attack is now beyond Salesloft-Salesforce integrations. We provide our prior general information on the attack below, along with the most recent update.

Salesloft Drift is a cloud-based sales engagement platform using artificial intelligence, with dozens of AI agents to do things such as account research, person research, buyer identification, and the like. Drift enables sales teams to automate workflows and integrate with Salesforce instances. Typically, the platform has website visitor and customer contact information, and perhaps more information, to drive website engagement with agentic AI insights.

Company engineers are investigating a suspected compromise of a Salesloft Drift application programming interface (API) key that may enable threat actors to access data integrated with some customer relationship manager (CRM) tenants.

Threat actors were observed attempting to exploit exposed API keys, creating the potential for unauthorized access to data shared between Drift and connected systems. In addition, threat actors are specifically exporting CRM data and searching for information such as API keys, passwords, and other credentials. These credentials and keys may allow access to additional data within other software-as-a-service (SaaS) environments or on-premises systems. Mandiant's Incident Response team published a security update on Aug. 26 attributing this attack to the threat group UNC6395.

In response to this activity, Salesloft revoked Drift integrations as a precautionary measure, thereby interrupting the ability for further unauthorized access to occur through the API linkage. Salesloft has proactively revoked Drift integrations with Salesforce to safeguard against potential unauthorized access, but as discussed below, it appears that the attack is now broader than this CRM system.

What you should do

First, call your IT team and see if your company has an integration with the Drift application with any CRM. If it does, then as a potentially affected company, you should review and rotate any API keys tied to Drift or your CRM and monitor system logs for unusual activity. Engineers are continuing to investigate the root cause, and guidance may evolve as additional information becomes available. Given the prevalence of AI integrations, we expect to see more breaches regarding vendors using AI-based technologies. We will continue to monitor this trend as a practice and discuss securing other AI-based platforms and integrations with you. For further guidance or assistance, please contact our team.

UPDATED GUIDANCE:

Mandiant's Incident Response team published a security update on Aug. 28, confirming that the scope of the compromise is broader than initially believed and is not limited to Drift's integration with Salesforce. At this stage, any integration involving Drift should be considered potentially compromised.

Engineers from Mandiant, part of Google Cloud, have identified that Open Authorization (OAuth) tokens issued to the Drift email application were also abused in connection with Google Workspace. As a precaution, Google has revoked the affected tokens and disabled the ability for Drift to integrate with Google Workspace. Salesforce and Salesloft had previously taken similar steps by revoking all active tokens tied to the Drift application. Salesloft has also published updated guidance discussing Drift API integrations, and provided a list of third-party platforms capable of integration with Drift.

This is an evolving situation, and guidance may change as additional findings are confirmed. We recommend that organizations review any existing Drift integrations, revoke and rotate associated credentials, and continue to monitor for updates.

Contacts

Please contact the listed attorneys for further information on the matters discussed herein.

AMY S. MUSHAHWAR
Partner
Chair, Data, Privacy & Cybersecurity
T: 202.753.3825
amushahwar@lowenstein.com

KATHLEEN A. MCGEE
Partner
T: 646.414.6831
kmcgee@lowenstein.com

CAIRON S. OVERTON
Counsel
T: 202.753.3747
coverton@lowenstein.com

This Alert has been prepared by Lowenstein Sandler LLP to provide information on recent legal developments of interest to our readers. It is not intended to provide legal advice for a specific situation or to create an attorney-client relationship. Lowenstein Sandler assumes no responsibility to update the Alert based upon events subsequent to the date of its publication, such as new legislation, regulations and judicial decisions. You should consult with counsel to determine applicable legal requirements in a specific fact situation. Attorney Advertising.