Data, Privacy & Cybersecurity

August 27, 2025

Salesforce Users: Organizations Using the Salesloft Drift AI Chat Agent with Salesforce Must Check Their Presence for Compromise

By Amy S. Mushahwar, Kathleen A. McGee, Cairon S. Overton, and Tricia Y. Wagner CIPP/US, CISSP, CISA

Salesloft issued a security notification on August 26 regarding its Drift application. It appears to be a broad opportunistic attack on Salesloft/Drift instances integrated with Salesforce tenants. Salesloft issued updates late last week.

What is Salesloft Drift?

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.

Impact appears to be limited to Salesforce tenants integrated with Salesloft Drift

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 Salesforce tenants. Salesloft has indicated that customers that do not integrate their data with Salesforce are not impacted by this campaign.

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 Salesforce case 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 August 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.

What you should do

First, call your IT team and see if your company has a Salesforce integration with the Drift application. If it does, then as a potentially affected company, you should review and rotate any API keys tied to Drift or Salesforce 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.

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

TRICIA Y. WAGNER CIPP/US, CISSP, CISA
Counsel
T: 202.753.3658
twagner@lowenstein.com

NEW YORK   PALO ALTO   NEW JERSEY   UTAH   WASHINGTON, D.C