Salesloft Drift supply chain attack leads to widespread data theft

September 10, 2025

Robert Duffy | Stephen E. Reynolds | Katelyn N. Ringrose | David Sorenson

Summary

Threat actors stole authentication tokens for Salesloft Drift, a popular marketing automation tool, leading to widespread data exfiltration from Salesforce customer instances that occurred mostly between August 8 and 18, 2025. Some affected companies believe that the threat actors targeted customer contact information and customer support information to use in subsequent attacks.

This client alert outlines the incident and provides actionable recommendations to help clients protect themselves.

In Depth

Salesloft confirmed that threat actors accessed Salesloft's development platform between March and June 2025 and stole the OAuth tokens that connect Salesloft Drift to various applications, including Salesforce and Google Workspace. According to Google Threat Intelligence Group (GTIG), the threat actors exfiltrated data from Salesforce customer instances between August 8 and 18, 2025. GTIG also reports that threat actors used OAuth credentials to access a small number of Google Workspace email accounts.

Numerous affected companies report that the affected data includes business contact information, customer relationship management information, and/or customer support information. Some companies have reported that the affected customer support information includes potentially sensitive information, such as system configurations, passwords, Application Programming Interface (API) keys, and other secrets.

Security tips

GTIG recommends that Drift customers take immediate action to review all third-party integrations connected to their Drift instance, revoke and rotate credentials for those applications, and investigate all connected systems for signs of unauthorized access. GTIG's detailed instructions and Indicators of Compromise (IOCs) are available on Google's blog. An FBI Flash report on the Drift campaign provides additional IOCs.

Clients should assess whether their vendors send or receive sensitive information –such as configuration information, credentials, and API keys – through standard communications channels. If so, they may consider asking the vendor whether this information is stored in any application that is connected to Salesloft Drift.

We urge all clients to take extra precautions against phishing, scams, and social engineering attacks.

- Consider warning your vendor-facing employees that their contact information may have been compromised.
- To help protect against the impersonation of your company and employees, consider a brand protection service to proactively identify and take down infringing domains and URLs.
- Protect against invoice and funds transfer fraud by informing your customers in writing about how you will notify them of any updates to your banking information and how they can confirm banking instructions. Additionally, provide detailed instructions to your accounts payable team on how to confirm payment instructions from vendors.

To reduce your exposure to future supply chain attacks, consider the following precautions.

- Avoid transmitting passwords, encryption keys, and other secrets through standard support channels, or use an additional layer of end-to-end encryption, such as PGP encryption.
- Review the configuration of your cloud applications and third-party integrations. Okta recommends inbound IP restrictions and client verification with DPoP (Demonstrating Proof of Possession), as described in their article on the subject.

If you believe you or your vendors were affected by the Salesloft Drift campaign, McDermott Will & Schulte can advise you on next steps. For more information, please contact your regular lawyer or one of the authors.

Get In Touch

Robert Duffy	Stephen E. Reynolds	Katelyn N. Ringrose	David Sorenson
View Profile	View Profile	View Profile	View Profile