Google warns Salesloft breach impacted some Workspace accounts - Aga

Data: 2025-08-28 22:55:06

Autor: Inteligência Against Invaders

Google now reports that the Salesloft Drift breach is larger than initially thought, warning that

attackers also used stolen OAuth tokens to access a small number of Google Workspace email

accounts in addition to stealing data from Salesforce instances.

“Based on new information identified by GTIG, the scope of this compromise is not exclusive to the Salesforce integration with Salesloft Drift and impacts other integrations,’ warns Google.

“We now advise all Salesloft Drift customers totreat any and all authentication tokens stored in or connected to the Drift platform as potentially compromised.”

The campaign, tracked by Google Threat Intelligence (Mandiant) as UNC6395, was first disclosed on August 26 after attackers stole OAuth tokens for Salesloft’s Drift AI chat integration with Salesforce. The threat actors used these tokens to gain access to customer Salesforce instances, where they executed queries against Salesforce objects, including the Cases, Accounts, Users, and Opportunities tables.

This data allowed the attackers to scan customer support tickets and messages for sensitive information, such as AWS access keys, Snowflake tokens, and passwords that could be used to breach further cloud accounts, likely for future extortion.

In an update published today, Google confirmed that the compromise was more significant than initially believed and not limited to Salesforce integrations.

The investigation revealed that OAuth tokens for the “Drift Email” integration were also compromised, and on August 9, the threat actors utilized them to access the email of a “very small number” of Google Workspace accounts that were directly integrated with Drift.

Google emphasized that no other accounts in those domains were impacted and that there has been no compromise of Google Workspace or Alphabet itself.

The stolen tokens have since been revoked, and customers have been notified. Google also disabled the integration between Salesloft Drift Email and Google Workspace while they investigate the breach.

Google is now urging all organizations using Drift to treat every authentication token stored in or connected to the platform as compromised. This warning advises customers to revoke and rotate credentials for those applications and investigate all connected systems for signs of unauthorized access.

The company also recommends reviewing all third-party integrations associated with Drift instances, searching for exposed secrets, and resetting any found credentials in case they have been compromised.

Salesloft also updated its advisory on August 28, stating that Salesforce has disabled Drift integrations with Salesforce, Slack, and Pardot until an investigation is completed.

The company has now engaged Mandiant and Coalition to assist with this investigation.

[IMAGEM REMOVIDA]