# Ataque à cadeia de suprimentos atinge Zscaler via Salesloft Drift, vazando

Data: 2025-09-01 19:00:20

Autor: Inteligência Against Invaders

## Ataque à cadeia de suprimentos atinge Zscaler via Salesloft Drift, vazando informações do cliente

## A violação do Zscaler vinculada ao ataque Salesloft Drift expôs dados do Salesforce, vazando informações do cliente e detalhes do caso de suporte em um comprometimento da cadeia de suprimentos.

Zscaler divulga uma violação de dados que está ligada ao recente Ataque Salesloft Drift. O fornecedor de segurança cibernética confirmou que foi afetado por uma campanha direcionada ao Salesloft Drift, um SaaS de marketing integrado ao Salesforce. Os agentes de ameaças roubaram tokens OAuth da empresa, o incidente afetou vários clientes da Salesforce, incluindo o Zscaler. Os invasores obtiveram acesso não autorizado às credenciais do Drift, permitindo visibilidade limitada de algumas das informações do Salesforce da Zscaler. A empresa ressaltou que seus produtos, serviços e infraestrutura central não foram comprometidos.

*“Como parte desta campanha, atores não autorizados obtiveram acesso às credenciais do Salesloft Drift de seus clientes, incluindo o Zscaler. Após uma revisão detalhada como parte de nossa investigação em andamento, determinamos que essas credenciais permitiram acesso limitado a algumas informações do Salesforce da Zscaler.” lê o Consultivo publicado pela Zscaler. “Após uma extensa investigação, a Zscaler atualmente não encontrou evidências que sugiram o uso indevido dessas informações.”*

As informações expostas no incidente são os detalhes de contato comercial comumente disponíveis para pontos de contato e conteúdo específico relacionado ao Salesforce, incluindo: nomes, endereços de email comercial, cargos, números de telefone, detalhes regionais/de localização, licenciamento de produtos Zscaler e informações comerciais, conteúdo de determinados casos de suporte.

A Zscaler confirmou que revogou o acesso ao Salesforce da Drift, alternou os tokens de API, lançou uma investigação conjunta com a Salesforce, adicionou salvaguardas, revisou fornecedores terceirizados e reforçou a autenticação de suporte ao cliente para reduzir os riscos de phishing.

A empresa pede aos clientes que permaneçam vigilantes contra tentativas de phishing e ataques de engenharia social, apesar do impacto limitado e sem evidências de uso indevido.

Na semana passada, o Google Divulgados que oViolação do Salesloft Drift OAuthé mais amplo do queForças Armadas, afetando todas as integrações. GTIG e Mandiant aconselham todos os clientes a tratar os tokens conectados como comprometidos. Os invasores usaram tokens OAuth roubados para acessar alguns e-mails do Google Workspace em 9 de agosto de 2025, por meio da integração

do Drift Email. O Google enfatizou que isso não era um comprometimento do Workspace em si, e apenas contas integradas ao Salesloft estavam em risco, sem acesso a outras contas de clientes.

*“Com base em novas informações identificadas pelo GTIG, o escopo desse comprometimento não é exclusivo da integração do Salesforce com o Salesloft Drift e afeta outras integrações. Agora aconselhamos todos os clientes do Salesloft Drift a tratar todo e qualquer token de autenticação armazenado ou conectado à plataforma Drift como potencialmente comprometido.” lê oatualizaçãopublicado pelo Google Threat Intelligence Group (GTIG).*

*“Em 28 de agosto de 2025, nossa investigação confirmou que o ator também comprometeu tokens OAuth para a integração “Drift Email”. Em 9 de agosto de 2025, um agente de ameaças usou esses tokens para acessar e-mails de um número muito pequeno de contas do Google Workspace. As únicas contas que foram potencialmente acessadas foram aquelas que foram configuradas especificamente para integração com o Salesloft; o ator não teria sido capaz de acessar nenhuma outra conta no domínio do Workspace de um cliente.”*

O Google já notificou os usuários afetados e revogou os tokens OAuth do Drift Email, desativou sua integração com o Workspace e pediu aos usuários do Salesloft Drift que revisassem as integrações, alternassem as credenciais e verificassem se há violações.

Na semana passada, pesquisadores do Google Threat Intelligence Group e da Mandiantanunciadoque investigaram uma campanha de roubo de dados em larga escaladestinado a hackeara plataforma de automação de vendasVendasloftpara roubar OAuth e atualizar tokens associados ao agente de bate-papo de inteligência artificial (IA) Drift.

Os especialistas descobriram que o agente da ameaça UNC6395 roubado tokens OAuth via Salesloft Drift, exfiltrando dados do Salesforce entre 8 e 18 de agosto de 2025, para coletar credenciais como chaves de acesso da AWS (AKIA) e tokens Snowflake.

*“Começando em 8 de agosto de 2025 até pelo menos 18 de agosto de 2025, o ator segmentou instâncias de clientes do Salesforce por meio de tokens OAuth comprometidos associados aoDeriva Salesloftaplicativo de terceiros.” lê o***relatório***publicado pelo grupo Google TIG. “O ator exportou sistematicamente grandes volumes de dados de várias instâncias corporativas do Salesforce.”*

UNC6395 roubou dados do Salesforce, levando o GTIG a aconselhar tratá-los como credenciais comprometidas e rotativas. O agente da ameaça excluiu trabalhos de consulta para evitar a detecção. O Google recomenda revisões de registro, revogação de chaves e rotação de credenciais para avaliar o comprometimento.

A Salesloft alertou que hackers exploraram as credenciais OAuth no aplicativo Drift para roubar dados do Salesforce (Casos, Contas, Usuários, Oportunidades). Em 20 de agosto de 2025, revogou todas as conexões Drift-Salesforce, enfatizando que os usuários que não são do Salesforce não são afetados. Os administradores são aconselhados a autenticar novamente as integrações do Salesforce, e os clientes afetados foram notificados, embora a escala total ainda não esteja clara.

*“De 8 a 18 de agosto de 2025, um agente de ameaças usou credenciais OAuth para exfiltrar dados das instâncias do Salesforce de nossos clientes. Todos os clientes afetados foram notificados.” lê oAtualização de segurança do Drift/Salesforcepublicado pela Salesloft. “As descobertas iniciais mostraram que o objetivo principal do ator era roubar credenciais, concentrando-se especificamente em informações confidenciais, como chaves de acesso da AWS, senhas e tokens de acesso*

*relacionados ao Snowflake. Determinamos que esse incidente não afetou os clientes que não usam nossa integração Drift-Salesforce.”*

A Salesforce disse que apenas um pequeno número de clientes foi afetado devido a uma conexão de aplicativo comprometida. Trabalhando com a Salesloft, ela revogou tokens, retirou o Drift do AppExchange e notificou os usuários afetados.

Siga-me no Twitter:@securityaffairseLinkedineMastodonte

PierluigiPaganini

(Assuntos de Segurança–hacking,Salesloft)