Violação de dados da Zscaler expõe informações do cliente após compror

Data: 2025-09-01 22:53:30

Autor: Inteligência Against Invaders

A empresa de segurança cibernética Zscaler alerta que sofreu uma violação de dados depois que os agentes de ameaças obtiveram acesso à sua instância do Salesforce e roubaram informações do cliente, incluindo o conteúdo de casos de suporte.

Este aviso segue o compromisso de SalesloftDrift, um agente de bate-papo de IA que se integra ao Salesforce, no qual os invasores roubaram OAuth e atualizaram tokens, permitindo que eles obtivessem acesso aos ambientes Salesforce do cliente e exfiltrassem dados confidenciais.

Em um comunicado, a Zscaler diz que sua instância do Salesforce foi afetada por esse ataque à cadeia de suprimentos, expondo as informações dos clientes.

“Como parte desta campanha, atores não autorizados obtiveram acesso às credenciais do Salesloft Drift de seus clientes, incluindo o Zscaler”, diz o Zscaler Consultoria da 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.”

As informações expostas incluem o seguinte:

- Nomes
- Endereços de e-mail comerciais
- Cargos
- Números de telefone
- Detalhes regionais/locais
- Licenciamento de produtos Zscaler e informações comerciais
- Conteúdo de determinados casos de suporte

A empresa enfatiza que a violação de dados afeta apenas sua instância do Salesforce e produtos, serviços ou infraestrutura noZscaler.

Embora a Zscaler afirme que não detectou nenhum uso indevido dessas informações, ela recomenda que os clientes permaneçam vigilantes contra possíveis ataques de phishing e engenharia social que possam explorar essas informações.

A empresa também diz que revogou todas as integrações do Salesloft Drift em sua instância do Salesforce, alternou outros tokens de API e está conduzindo uma investigação sobre o incidente.

A Zscaler também fortaleceu seu protocolo de autenticação do cliente ao responder às chamadas de suporte ao cliente para se proteger contra ataques de engenharia social.

O Google Threat Intelligence alertou na semana passada que um agente de ameaças, rastreado como UNC6395, está por trás dos ataques, roubando casos de suporte para coletar tokens de autenticação, senhas e segredos compartilhados pelos clientes ao solicitar suporte.

“O GTIG observou UNC6395 visando credenciais confidenciais, como chaves de acesso (AKIA) da Amazon Web Services (AWS), senhas e tokens de acesso relacionados ao Snowflake”,relatórios do Google.

“UNC6395 demonstrou consciência de segurança operacional excluindo trabalhos de consulta, no entanto, os logs não foram afetados e as organizações ainda devem revisar os logs relevantes para evidências de exposição de dados.”

Mais tarde, foi revelado que o ataque à cadeia de suprimentos da Salesloft não afetou apenas a integração do Drift Salesforce, mas também o Drift Email, que é usado para gerenciar respostas de e-mail e organizar bancos de dados de CRM e automação de marketing.

O Google alertou na semana passada que os invasores também usaram tokens OAuth roubados para acessar contas de e-mail do Google Workspace e ler e-mails como parte dessa violação.

O Google e o Salesforce desativaram temporariamente suas integrações do Drift enquanto aguardam a conclusão de uma investigação.

Alguns pesquisadores disseram ao BleepingComputer que acreditam que o compromisso Salesloft Drift se sobrepõe aoataques recentes de roubo de dados do Salesforce pelo grupo de extorsão ShinyHunters.

Desde o início do ano, os agentes de ameaças têm conduzido ataques de engenharia social para violar instâncias do Salesforce e baixar dados.

Durante esses ataques, os agentes de ameaças realizam phishing de voz (vishing) para induzir os funcionários a vincular um aplicativo OAuth malicioso às instâncias do Salesforce de sua empresa.

Uma vez vinculados, os agentes de ameaças usaram a conexão para baixar e roubar os bancos de dados, que foram usados para extorquir a empresa por e-mail.

DesdeO Google relatou os ataques pela primeira vez em junho, várias violações de dados foram vinculadas aos ataques de engenharia social, incluindoO próprio Google,Cisco,Seguro de Agricultores,Dia de trabalho,Adidas,Qantas,Allianz Lifee as filiais da LVMHLouis Vuitton,DioreTiffany & Co.

[IMAGEM REMOVIDA]