A vulnerabilidade do token de senha FlowiseAI permite a aquisição da con

Data: 2025-09-15 07:59:00

Autor: Inteligência Against Invaders

A vulnerabilidade acrítica em FlowiseIA foi descoberta que permite que os invasores assumam as

contas de usuário com um esforço mínimo.

A falha, rastreada comoCVE-2025-58434afeta as implantações FlowiseAI hospedadas e auto-hospedadas na nuvem, representando riscos significativos para as organizações usando esta plataforma de automação de fluxo de trabalho de IA.

Número cve	Produto afetado	Tipo de vulnerabilidade	CVSS 3.1 Pontuação
CVE-2025-58434	Flowiseai (pacote NPM Flowise)	Divulgação de token de senha não autenticada	9.8 (crítico)

Falha crítica de segurança no mecanismo de redefinição de senha

A vulnerabilidade está dentro da funcionalidade de redefinição de senha do FlowIeAI, especificamente a/api/v1/conta/esquecia-passaWordEndPons, conforme a relatório pelo pesquisador de segurança.

Em vez de seguir as práticas seguras enviando apenas tokens de redefinição por e -mail, o Systems retorna as informações confidenciais do usuário na resposta da API, incluindo tokens de redefinição de senha válida.

Quando um invasor solicita uma redefinição de senha para qualquer endereço de email, o sistema responde com detalhes abrangentes do usuário, incluindo o ID do usuário, nome, email, credenciais de hash e, mais criticamente, um validTeptokenthat pode ser usado imediatamente para redefinir a senha da conta de destino.

Essa falha de design ignora completamente o mecanismo de segurança pretendido da verificação baseada em email.

A vulnerabilidade afeta as versões FlowIeAI abaixo de 3.0.5, com nenhum patches atualmente disponíveis. A questão afeta o serviço em nuvem em cloud.flowiseAI.com e implantações auto-hospedadas que expõem os terminais de API vulneráveis.

Explorar essa vulnerabilidade requer apenas o endereço de e -mail da vítima, que os atacantes podem adivinhar ou descobrir através do reconhecimento.

O processo de ataque envolve apenas dois Http solicitações. Primeiro, os invasores enviam uma solicitação de postagem para o terminal esquecido-passa-palavra com o endereço de e-mail do alvo. O sistema responde com um token de redefinição válido em vez de simplesmente confirmar a

solicitação.

Segundo, os invasores usam esse token exposto no terminal de redefinição-passanha para definir uma nova senha para a conta da vítima.

Nenhuma verificação de email ou interação do usuário é necessária, tornando este um ataque completamente silencioso que as vítimas podem não notar até que tentem fazer login.

A vulnerabilidade recebeu a pontuação do ACVSS de 9,8, indicando gravidade crítica. A pontuação alta reflete a facilidade de exploração, pois não requer autenticação, nenhuma interação do usuário e possui baixa complexidade de ataque, fornecendo acesso completo às contas de usuário.

Essa falha permite que os invasores comprometam qualquer conta, incluindo contas administrativas ou de alto privilégio, potencialmente levando a violações de dados, Acesso não autorizado a fluxos de trabalho sensíveis de IA e compromisso organizacional completo.

O impacto da vulnerabilidade se estende além das contas individuais, pois as contas de administração comprometidas podem fornecer acesso a implantações organizacionais inteiras e dados associados.

As organizações que usam o FlowIeAI devem implementar imediatamente o monitoramento para obter atividades suspeitas de redefinição de senha e considerar restringir temporariamente o acesso à plataforma até que os patches estejam disponíveis.

Encontre esta história interessante! Siga -nosLinkedIneXPara obter mais atualizações instantâneas.