GitLab corrige vulnerabilidade crítica CVE-2025-6454

Data: 2025-09-18 16:16:04

Autor: Inteligência Against Invaders

Redazione RHC**:18 Setembro 2025 17:41**

A plataforma de desenvolvimento colaborativo GitLab anunciou A correção para uma vulnerabilidade crítica, identificada como CVE-2025-6454. O problema afetou as instalações do servidor das edições Community e Enterprise e permitiu que solicitações fossem feitas a recursos internos por meio de cabeçalhos de webhook especialmente criados.

O ataque exigiu uma conta com **Privilégios mínimos de desenvolvedor** e nenhuma intervenção de outros usuários foi necessária.

O bug recebeu uma alta pontuação CVSS de 8,5 em 10. Afetou versões *16.11 a 18.1.6, 18.2 a 18.2.6 e 18.3 a 18.3.2.* As correções foram incluídas na versão 18.3.2, lançada em 10 de setembro. O GitLab enfatizou que o problema foi descoberto por meio de um programa de caça a bugs e que o relatório foi escrito por um pesquisador usando o pseudônimo “PPEE “.

A vulnerabilidade era única na medida em que **permitido ignorando as restrições de isolamento de rede.** Solicitações *podem ser enviados para proxies internos, serviços de metadados ou APIs locais.* Isso era visível em logs de eventos por meio de cabeçalhos HTTP não padrão e solicitações para endereços atípicos. Especialistas alertam que tais ataques podem levar ao vazamento de dados confidenciais e comprometer a integridade da infraestrutura.

No momento da publicação, não há exploração disponível publicamente, nem há evidências de exploração real. No entanto, o perigo potencial é alto: a descrição afirma que a vulnerabilidade afeta a confidencialidade, disponibilidade e integridade dos dados.

Os desenvolvedores são aconselhados a **atualize o GitLab para as versões 18.1.6, 18.2.6 ou 18.3.2 ou posteriores** O mais rápido possível. Também recomendamos revisar as configurações do webhook e desabilitar o uso de *cabeçalhos personalizados, se os usuários puderem defini-los.*

Para implantações baseadas em proxy reverso, recomendamos *restringindo o acesso do GitLab a recursos internos*. Também recomendamos monitorar logs em busca de solicitações suspeitas e segmentar sua rede para evitar acesso indesejado.

Redação
A equipe editorial da Red Hot Cyber é composta por um grupo de indivíduos e fontes anônimas que colaboram ativamente para fornecer informações e notícias antecipadas sobre segurança cibernética e computação em geral.

Lista degli articoli