TLP: CLEAR


# BOLETIM DE SEGURANÇA

## GitLab lança atualizações para corrigir vulnerabilidades de alta gravidade

heimdall
security research

Acesse a nossa nova comunidade através do WhatsApp!

**Heimdall Security Research**


Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

**Boletins de Segurança – Heimdall**

# SUMÁRIO

# 1 SUMÁRIO EXECUTIVO

O **GitLab** divulgou recentemente a disponibilização de importantes atualizações de segurança para suas edições **Community Edition (CE)** e **Enterprise Edition (EE)**. As versões mais recentes, identificadas como *17.6.2*, *17.5.4* e *17.4.6*, trazem correções para múltiplas vulnerabilidades classificadas como de alta gravidade.

## 2 INFORMAÇÕES SOBRE AS VULNERABILIDADES

As novas atualizações do GitLab corrigem dois problemas graves que representavam altos riscos significativos de segurança. Essas correções são parte de um esforço contínuo para proteger usuários contra ameaças emergentes e garantir a integridade das operações na plataforma.

Um deles envolve a injeção de cabeçalhos de **Registro de Erros de Rede (NEL)** nas respostas do proxy do Kubernetes. Essa vulnerabilidade, catalogada como **CVE-2024-11274**, afeta as versões do *GitLab CE/EE* entre *16.1* e *17.4.6*, *17.5* e *17.5.4*, bem como *17.6* até *17.6.2*. A falha poderia ser explorada para realizar a exfiltração de dados de sessão por meio do abuso de fluxos OAuth. O problema foi solucionado nas versões mais recentes, demonstrando o compromisso do GitLab com a segurança.

Outro ponto crítico tratado foi uma vulnerabilidade que permitia ataques de **Negação de Serviço (DoS)**. Ela poderia ser explorada enviando solicitações não autenticadas para *arquivos diff* durante uma confirmação ou solicitação de mesclagem. Identificada como **CVE-2024-8233**, essa falha impactava as versões do *GitLab CE/EE* de *9.4* até *17.4.6*, *17.5* até *17.5.4* e *17.6* até *17.6.2*. Esse vetor de ataque poderia ser utilizado para interromper significativamente os serviços, mas agora está mitigado com os patches mais recentes, reforçando a estabilidade e a confiabilidade da plataforma.

Devido a explorações anteriores de falhas de segurança no GitLab por atores maliciosos, esta vulnerabilidade requer uma notável atenção.

# 3 RECOMENDAÇÕES

O GitLab reforça a necessidade de atualizar imediatamente todas as instalações autogerenciadas. É importante destacar que o GitLab[.]com já opera com a versão corrigida, e os clientes que utilizam ambientes dedicados ao GitLab não precisam realizar nenhuma ação adicional.

# 4 REFERÊNCIAS


- **Heimdall *by* ISH Tecnologia**
- **GitLab**
- **CVE**
- **Gbhackers**


# 5 AUTORES


- **Rafael de Moura Salomé**

heimdall
security research
A DIVISION OF ISH