



BOLETIM DE SEGURANÇA

GitLab lança atualizações para corrigir vulnerabilidades
de alta gravidade

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



ISH

CONTAS DO FACEBOOK SÃO INVADIDAS POR EXTENSÕES MALICIOSAS DE NAVEGADORES

Descoberto recentemente que atores maliciosos utilizam extensões de navegadores para realizar o roubo de cookies de sessões de sites como o Facebook. A extensão maliciosa é oferecida como um anexo do ChatGPT...

BAIXAR



ISH

ALERTA PARA RETORNO DO MALWARE EMOTET!

O malware Emotet após permanecer alguns meses sem operações retornou com outro meio de propagação, via OneNote e também dos métodos já conhecidos via Planilhas e Documentos do Microsoft Office...

BAIXAR



ISH

GRUPO DE RANSOMWARE CLOP EXPLORANDO VULNERABILIDADE PARA NOVAS VÍTIMAS

O grupo de Ransomware conhecido como ClOp está explorando ativamente a vulnerabilidade conhecida como CVE-2023-0669, na qual realizou o ataque a diversas organizações e expôs os dados no site de data leaks...

BAIXAR

SUMÁRIO

1	Sumário Executivo	4
2	Informações sobre as vulnerabilidades.....	5
3	Recomendações.....	6
4	Referências	7
5	Autores.....	7

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