BOLETIM DE SEGURANÇA

Vulnerabilidade CVE-2024-5655 crítica do GitLab permite que invasores executem pipelines como qualquer usuário

heimdall
security research
A DIVISION OF ISH

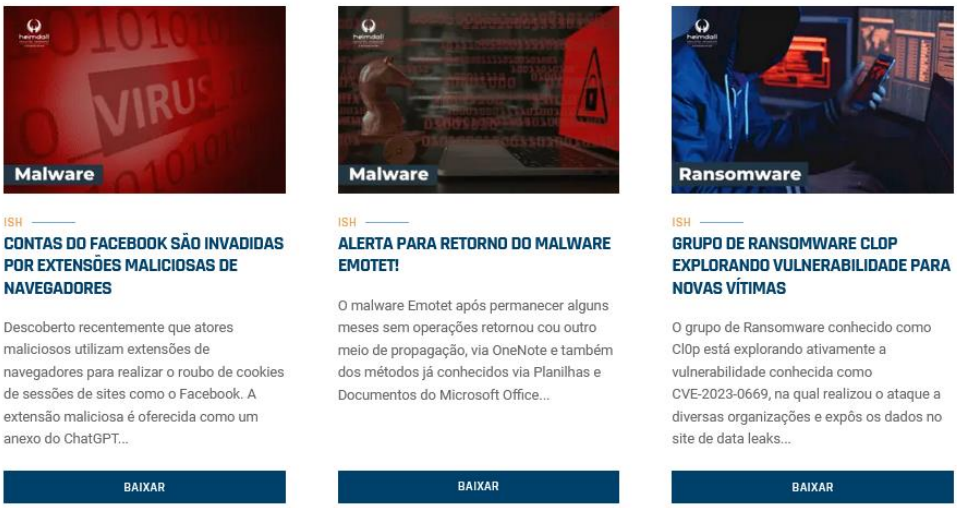
TLP: CLEAR

Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso **X**.

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

Recentemente a GitLab informou sobre a vulnerabilidade CVE-2024-5655 que está afetando certas versões dos produtos GitLab Community e Enterprise Edition, que podem ser exploradas para executar pipelines como qualquer usuário.

2 INFORMAÇÕES SOBRE A VULNERABILIDADE

A vulnerabilidade CVE-2024-5655 classificada como crítica com gravidade de 9,6 de 10, pode ser explorada por um invasor para disparar um pipeline como outro usuário.

Os pipelines do GitLab, parte integrante do sistema de Integração Contínua/Implantação Contínua (CI/CD), permitem a execução automática de processos e tarefas para construir, testar ou implantar alterações de código. A vulnerabilidade afeta todas as versões do GitLab CE/EE de 15.8 a 16.11.4, de 17.0.0 a 17.0.2 e de 17.1.0 a 17.1.0. Além disso, a atualização mais recente do GitLab também resolve outros 13 problemas de segurança, três dos quais são classificados como gravidade alta, com:

- CVE-2024-4901: Que trata-se de uma vulnerabilidade de XSS armazenado que foi descoberta no GitLab CE/EE. Ela afeta todas as versões a partir de 16.9 antes de 16.11.5, a partir de 17.0 antes de 17.0.3, e a partir de 17.1 antes de 17.1.1. A vulnerabilidade poderia ser importada de um projeto com notas de confirmação maliciosas.

- CVE-2024-4994: Sendo uma vulnerabilidade CSRF na API GraphQL do GitLab. Ela permite que invasores executem mutações arbitrárias do GraphQL enganando usuários autenticados para fazer solicitações indesejadas. Isso pode levar à manipulação de dados e operações não autorizadas.

- CVE-2024-6323: Esta vulnerabilidade é uma falha de autorização no recurso de pesquisa global do GitLab. Ela permite que invasores visualizem resultados de pesquisa de repositórios privados dentro de projetos públicos. Isso pode levar a vazamentos de informações e acesso não autorizado a dados confidenciais.

3 RECOMENDAÇÕES

Para corrigir a vulnerabilidade, o GitLab lançou as versões 17.1.1, 17.0.3 e 16.11.5 e aconselha os usuários a aplicarem as atualizações o mais rápido possível. A atualização traz duas mudanças significativas: os pipelines não serão mais executados automaticamente quando uma solicitação de mesclagem for redirecionada após a mesclagem de sua ramificação de destino anterior, e o CI_JOB_TOKEN agora está desabilitado por padrão para autenticação GraphQL a partir da versão 17.0.0.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **GitLab**
- **Bleepingcomputer**
- **NVD**

5 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH