ALERTA DE VULNERABILIDADE

GitLab alerta sobre instalação de atualização de segurança para falha crítica.

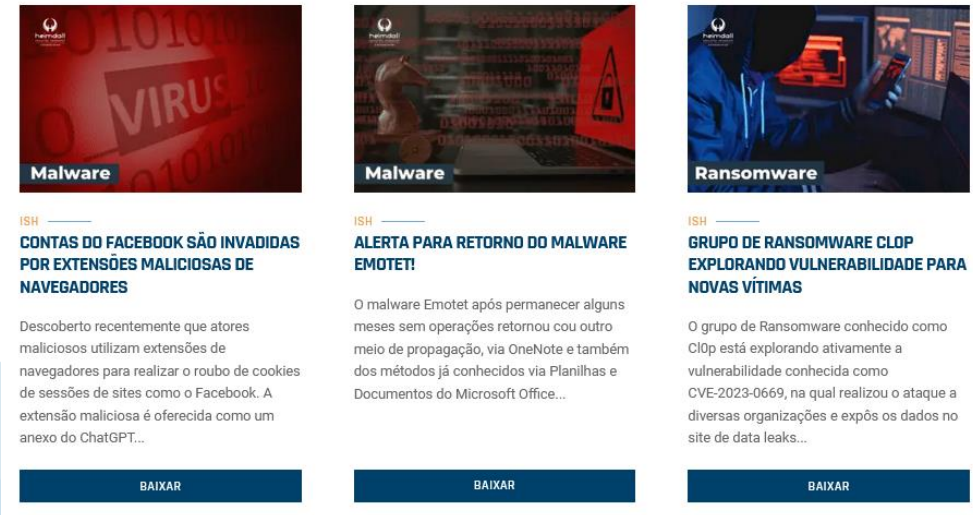
heimdall
security research
A DIVISION OF ISH

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

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



heimdall
security research

Sumário

1 FALHA DE SEGURANÇA CRÍTICA NO GITLAB

Recentemente o GitLab divulgou atualizações de segurança para resolver uma vulnerabilidade classificada como crítica, identificada como **CVE-2023-5009** (com uma pontuação CVSS de 9,6). Essa vulnerabilidade possibilita que um atacante execute pipelines em nome de outro usuário, a fragilidade reside no **GitLab EE** e afeta todas as versões a partir de **13.12** e **anteriores** a **16.2.7**, todas as versões a partir de **16.3 antes** de **16.3.4**.

2 EXTENSÃO DE VULNERABILIDADE

Em comunicado o GitLab informou que havia um desviou de uma vulnerabilidade média rastreada como CVE-2023-3932, a qual foi corrigida em agosto. Porém um pesquisador de segurança cibernética identificou uma maneira de contornar as proteções inicialmente implantadas e, ao fazê-lo, revelou um agravamento adicional que elevou a gravidade da falha para o nível crítico. Essencialmente, essa vulnerabilidade permite a um atacante se passar por um usuário, sem que o usuário tenha conhecimento ou concedido permissão, para executar uma série de tarefas automatizadas conhecidas como "**pipelines**". Isso abre a porta para invasores acessarem informações confidenciais ou abusarem das permissões associadas ao usuário que estão personificando, possibilitando a execução de código malicioso, modificações de dados indesejadas ou a ativação de eventos específicos no ambiente do GitLab.

Dado que o GitLab é uma ferramenta fundamental para a gestão de código e projetos, uma exploração bem-sucedida dessa vulnerabilidade poderia acarretar sérias consequências, incluindo a perda de propriedade intelectual, divulgação de dados sensíveis, comprometimento da cadeia de suprimentos e outros cenários de alto risco.

O comunicado oficial do GitLab enfatiza a extrema gravidade dessa vulnerabilidade e faz o pedido que os usuários a aplicarem de imediato as atualizações de segurança disponíveis como medida crucial para corrigir o problema e reduzir os riscos associados. A empresa resolveu a vulnerabilidade com o lançamento do 16.3.4 para Community Edition e 16.2.7 para Enterprise Edition.

3 RECOMENDAÇÕES

Devido a explorações por atores maliciosos já ocorridas no GitLab pela CVE-2021-22205, também classificada com crítica, informamos a necessidade da **atualização de segurança** informada neste relatório para proteção de eventuais riscos cibernéticos associados as vulnerabilidades.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- GitLab
- thehackernews
- NVD
- bleepingcomputer


heimdall
security research
A DIVISION OF ISH