BOLETIM DE SEGURANÇA

GitLab corrige vulnerabilidade crítica de autenticação SAML que permitia by-pass

heimdall
security research
A DIVISION OF ISH

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 cou 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 Cl0p 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

Lista de Figuras

1 SUMÁRIO EXECUTIVO

O GitLab disponibilizou atualizações de segurança para corrigir uma vulnerabilidade crítica de alta gravidade que permite o **bypass da autenticação SAML**. Essa falha afeta as instalações autogerenciadas do GitLab Community Edition (CE) e Enterprise Edition (EE). O Security Assertion Markup Language (SAML) é um protocolo de logon único (SSO) que permite que usuários utilizem as mesmas credenciais para acessar diversos serviços. A vulnerabilidade, identificada como **CVE-2024-45409**, decorre de problemas nas bibliotecas OmniAuth-SAML e Ruby-SAML, utilizadas pelo GitLab para gerenciar a autenticação baseada em SAML.

2 DETALHES SOBRE A VULNERABILIDADE

A falha ocorre quando a resposta **SAML** enviada por um provedor de identidade (IdP) ao GitLab apresenta uma configuração incorreta ou é manipulada. O problema reside em uma validação insuficiente de elementos críticos nas asserções SAML, como o *extern_uid*, usado para identificar exclusivamente usuários em diferentes sistemas. Com isso, um invasor pode enviar uma resposta SAML maliciosa, fazendo o GitLab reconhecê-lo como um usuário autenticado, contornando a autenticação SAML e obtendo acesso indevido à instância do GitLab.

Versões afetadas

- Todas as versões anteriores a 17.3.3, 17.2.7, 17.1.8, 17.0.8, 16.11.10 para GitLab Community Edition (CE) e Enterprise Edition (EE).

3 INDÍCIOS DE EXPLORAÇÃO COMPARTILHADA

Apesar do GitLab não ter confirmado que a vulnerabilidade foi explorada anteriormente, eles incluíram no boletim alguns indicadores de tentativas ou exploração bem-sucedida, sugerindo que agentes mal-intencionados podem já estar utilizando a falha em ataques.

Os sinais de tentativas ou explorações bem-sucedidas incluem:

- Erros relacionados a **RubySaml::ValidationError** (indicando tentativas falhas).
- Presença de valores **extern_uid** novos ou estranhos nos logs de autenticação (indicando tentativas bem-sucedidas).
- Informações ausentes ou incorretas nas respostas **SAML**.
- Múltiplos valores **extern_uid** associados a um único usuário (potencial sinal de comprometimento de conta).
- Autenticação SAML vinda de um **endereço IP desconhecido ou suspeito** em comparação com o padrão de acesso usual do usuário.


```
{"severity":"INFO","time":"2024-xx-
xx","correlation_id":"xx","meta.caller_id":"OmniauthCallbacksController#saml","meta.rem
ote_ip":"0.0.0.0","meta.feature_category":"system_access","meta.client_id":"ip/0.0.0.0"
,"message":"(SAML) saving user exploit-test-user@domain.com from login with admin
=\\u003e false, extern_uid =\\u003e exploit-test-user"}
```


Figura 1 – Exemplo de log de exploração bem-sucedida disponibilizado.

4 RECOMENDAÇÕES

As recomendações de segurança indicadas para a proteção desta vulnerabilidade são as seguintes:

- Atualização para a versão mais recente
- Para aqueles que não podem atualizar para uma versão segura imediatamente, o GitLab sugere habilitar a autenticação de dois fatores **(2FA)** para todas as contas e definir a opção de ignorar SAML 2FA como "**do not allow**."

5 REFERÊNCIAS

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

6 AUTORES

- **Ismael Pereira Rocha**

heimdall
security research
A DIVISION OF ISH