BOLETIM DE SEGURANÇA

Vulnerabilidade crítica no GitHub Enterprise Server com pontuação máxima

heimdall
security research
A DIVISION OF ISH

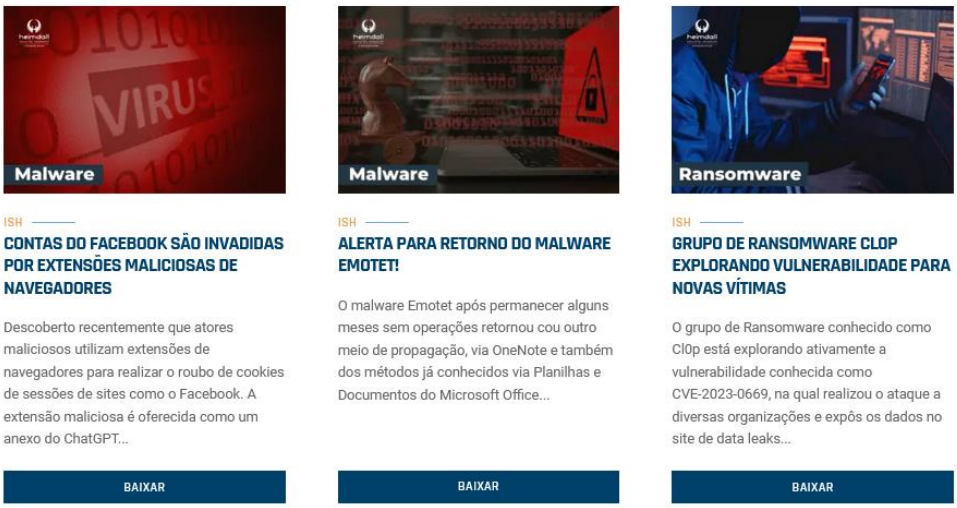
TLP: CLEAR

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

O GitHub implementou uma correção de segurança para a vulnerabilidade CVE-2024-4985 categorizada como crítica (com pontuação máxima de 10.0 no CVSS). Essa falha impactava as versões do GitHub Enterprise Server (GHES) que utilizavam o sistema de autenticação SAML para logon único (SSO).

2 INFORMAÇÃO SOBRE A VULNERABILIDADE

A vulnerabilidade CVE-2024-4985 possibilita um atacante criar uma resposta SAML falsificada, obtendo assim privilégios de administrador e acesso total e irrestrito ao conteúdo da instância, sem necessidade de autenticação prévia. O GitHub Enterprise Server (GHES), é uma solução do GitHub para auto-hospedagem, ideal para organizações que optam por manter seus repositórios em servidores próprios ou em um ambiente de nuvem privado.

O GitHub também notou que, por padrão, as asserções criptografadas não estão ativas, e a vulnerabilidade não impacta as instâncias que não empregam o logon único SAML (SSO) ou as que operam com autenticação SAML SSO, mas sem o uso de asserções criptografadas. A utilização de asserções criptografadas viabiliza que os gestores do site intensifiquem a proteção de uma instância GHES que opera com SAML SSO, ao codificar as comunicações enviadas pelo provedor de identidade SAML (IdP) no decorrer do procedimento de autenticação. Essa vulnerabilidade impacta somente as instâncias do GHES onde os administradores optaram por ativar as asserções criptografadas, uma vez que essa não é a configuração padrão do sistema. Foram implementadas correções para a vulnerabilidade e estão disponíveis nas versões 3.12.4, 3.11.10, 3.10.12 e 3.9.15 do GHEL, que foram disponibilizadas para os usuários no dia 20 de maio.

A atualização apresenta certas questões conhecidas que incluem, a exclusão de regras de firewall personalizadas, erros ignoráveis como “No such object” em serviços específicos e “mbind’, que são operação não permitida nos logs do MySQL, desbloqueio manual necessário para a conta de administrador raiz após bloqueio, exigindo acesso SSH, falhas no encaminhamento de log TLS, devido a pacotes de CA não reconhecidos pelo ghe-ssl-ca-certificate-install, perda de sincronização de horário em instâncias da AWS após reinicializações, logs de auditoria mostrando todos os IPs de clientes como 127.0.0.1 quando usando o cabeçalho X-Forwarded-For atrás de balanceadores de carga, problemas de renderização para arquivos .adoc grandes na interface web, embora acessíveis como texto simples, falhas potenciais na restauração de backup se o Redis não reiniciar adequadamente, rastreamento incorreto de contribuições em repositórios importados via ghe-migrator, falhas nos fluxos de trabalho do GitHub Actions para GitHub Pages, necessitando de comandos SSH específicos para correção.

3 RECOMENDAÇÕES

Apesar desses problemas, os que usam a configuração vulnerável (SAML SSO + asserções criptografadas) devem atualizar imediatamente para uma versão segura do GHEL.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **GitHub**
- **Thehackernews**
- **Bleepingcomputer**

5 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH