



BOLETIM DE SEGURANÇA

GitHub corrige falha crítica de segurança no Enterprise
Server



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](#)



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.....	8

1 SUMÁRIO EXECUTIVO

O GitHub lançou correções para resolver um conjunto de três falhas de segurança que afetam seu produto Enterprise Server, incluindo um bug crítico [CVE-2024-6800](#) CVSS: **9.5** que poderia ser explorado para obter privilégios de administrador do site.

2 INFORMAÇÕES SOBRE AS VULNERABILIDADES

CVE-2024-6800 em instâncias do GitHub Enterprise Server que utilizam autenticação SAML single sign-on (SSO) com IdPs específicos que utilizam XML de metadados de federação assinados e expostos publicamente, um invasor poderia forjar uma resposta SAML para provisionar e/ou obter acesso a uma conta de usuário com privilégios de administrador do site.

A subsidiária da Microsoft também abordou duas falhas de gravidade média:

- A [CVE-2024-7711](#): Uma vulnerabilidade de autorização incorreta que poderia permitir a um invasor atualizar o título, os responsáveis e os rótulos de qualquer problema dentro de um repositório público.
- A [CVE-2024-6337](#): Uma vulnerabilidade de autorização incorreta que poderia permitir a um invasor acessar conteúdos de problemas de um repositório privado usando um aplicativo GitHub com apenas permissões de leitura de conteúdos e escrita de pull requests.

Todas as três vulnerabilidades de segurança foram corrigidas nas versões **3.13.3, 3.12.8, 3.11.14 e 3.10.16** do **GHE**.

Em maio, o GitHub também corrigiu uma vulnerabilidade crítica de segurança (CVE-2024-4985) que poderia permitir acesso não autorizado a uma instância sem exigir autenticação prévia.

3 RECOMENDAÇÕES

Organizações que estão executando uma versão auto hospedada vulnerável do GHES são altamente recomendadas a [atualizar](#) para a versão mais recente para se proteger contra possíveis ameaças de segurança.

4 REFERÊNCIAS

- Heimdall by ISH Tecnologia
- [Github](#)
- [Thehackernews](#)
- [NVD](#)

5 AUTORES

- Leonardo Oliveira Silva



heimdall
security research

A DIVISION OF ISH