TLP: CLEAR

BOLETIM DE SEGURANÇA

Falhas de segurança no Git possibilitam o comprometimento de credenciais

heimdall
security research

Acesse a nossa nova comunidade através do WhatsApp!

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 INTRODUÇÃO EXECUTIVA

Recentemente, foram identificadas vulnerabilidades no Git e em seus auxiliares de credenciais que permitem que atacantes obtenham credenciais de usuários por meio de ataques denominados **Clone2Leak**. Essas falhas afetam ferramentas amplamente utilizadas, como ***GitHub Desktop***, ***Git LFS***, ***GitHub CLI/Codespaces*** e o ***Git Credential Manager***.

2 INFORMAÇÕES SOBRE AS VULNERABILIDADES

As vulnerabilidades exploradas pelo Clone2Leak estão relacionadas ao manuseio inadequado de solicitações de autenticação pelos auxiliares de credenciais do Git. Os auxiliares de credenciais são ferramentas que armazenam e recuperam credenciais de autenticação quando o Git interage com repositórios remotos, evitando a necessidade de inserir credenciais repetidamente. As falhas permitem que um atacante engane o Git para vazar credenciais armazenadas ao interagir com um repositório malicioso. Confira mais informações sobre as vulnerabilidades a seguir:

CVE-2025-23040

- Essa vulnerabilidade afeta o **GitHub Desktop** e ocorre devido ao manuseio inadequado de caracteres de controle em URLs. Atacantes podem explorar essa falha inserindo Carriage Return Smuggling (\r) em URLs maliciosas, resultando no vazamento de credenciais para servidores sob seu controle.

CVE-2024-50338

- Presente no **Git Credential Manager (GCM)**, essa falha permite que atacantes explorem a interpretação inadequada de caracteres de controle, como Carriage Return Smuggling (\r), usados para manipular fluxos de credenciais. Isso pode levar ao vazamento de informações sensíveis ao interagir com repositórios comprometidos.

CVE-2024-53263

- É uma vulnerabilidade identificada no **Git Large File Storage (LFS)**, relacionada ao manuseio inadequado de URLs ao solicitar credenciais. A falha ocorre porque o Git LFS não valida corretamente caracteres de controle embutidos (como \r ou \n) na URL antes de enviá-la ao auxiliar de credenciais do Git. Isso permite que um atacante insira caracteres maliciosos na URL, manipulando o fluxo de dados e obtendo credenciais sensíveis do usuário.

CVE-2024-53858

- É uma vulnerabilidade identificada na **GitHub CLI**, a ferramenta oficial de linha de comando do GitHub. Essa falha permite que tokens de autenticação sejam vazados ao clonar repositórios que contêm submódulos hospedados fora dos domínios *github.com* e *ghe.com*.

2.1 SISTEMAS E PRODUTOS AFETADOS

As vulnerabilidades afetam as seguintes ferramentas e versões:

- **GitHub Desktop**: Versão *3.3.15 e* anteriores.
- **Git LFS**: Versão *3.6.0 e* anteriores.
- **GitHub CLI/Codespaces**: Versão *2.62.0 e* anteriores.
- **Git Credential Manager**: Versão *2.6.0 e* anteriores.

2.2 IMPACTO DA VULNERABILIDADE

Os impactos das vulnerabilidades associadas ao ataque Clone2Leak incluem:

- Comprometimento de credenciais sensíveis
- Acesso não autorizado a repositórios
- Modificação maliciosa de códigos-fonte
- Distribuição de código malicioso
- Exfiltração de dados sensíveis

3 RECOMENDAÇÕES

Para mitigar os riscos associados às vulnerabilidades citadas neste relatório, é altamente recomendável que os usuários adotem as seguintes medidas:

Atualização imediata para as versões corrigidas das ferramentas afetadas:

- GitHub Desktop: versão *3.4.12* ou superior.
- Git LFS: versão *3.6.1* ou superior.
- GitHub CLI/Codespaces: versão *2.63.0* ou superior.
- Git Credential Manager: versão *2.6.1* ou superior.

Revisão de configurações:

- Verifique as configurações do Git e dos auxiliares de credenciais para garantir que não haja entradas desconhecidas ou suspeitas.

Cautela com repositórios desconhecidos:

- Evite clonar ou interagir com repositórios de fontes não confiáveis ou desconhecidas.

Monitoramento contínuo:

- Implemente práticas de monitoramento para detectar atividades suspeitas ou não autorizadas em seus repositórios e sistemas associados.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **GitHub**
- **NVD**
- **GMO Flatt Security**
- **Bleeping Computer**

5 AUTORES

- **Rafael Salomé**

heimdall
security research
A DIVISION OF ISH