



BULLETIN DE SECURITE

Titre	Vulnérabilités critiques dans les produits GitHub
Numéro de Référence	52202801/25
Date de Publication	28 Janvier 2025
Risque	Critique
Impact	Critique

Systemes affectés

- GitHub Desktop antérieure à 3.4.12
- Git Credential Manager antérieure à 2.6.1
- Git LFS antérieure à 3.6.1
- GitHub CLI antérieure à 2.63.0
- Git antérieure à v2.48.1 v2.47.2 v2.46.3 v2.45.3 v2.44.3 v2.43.6 v2.42.4 v2.41.3 v2.40.4

Identificateurs externes

- CVE-2024-53263, CVE-2024-50338, CVE-2025-23040,
- CVE-2024-5385, CVE-2024-5200, CVE-2024-5034

Bilan de la vulnérabilité

GitHub a publié des mises à jour de sécurité pour corriger plusieurs vulnérabilités critiques affectant les produits susmentionnés. L'exploitation réussie de ces vulnérabilités pourrait permettre à un attaquant d'obtenir un accès non autorisé aux informations d'identification Git des utilisateurs. Ces vulnérabilités, collectivement appelées « Clone2Leak », exploitent une mauvaise gestion des messages dans le protocole Git Credential.

Solution

Veillez se référer au bulletin de sécurité GitHub afin d'installer les nouvelles mises à jour.

Risque

- Contournement d'authentification
- Atteinte à la confidentialité des données

Référence

Bulletin de sécurité GitHub :

- <https://github.com/git-lfs/git-lfs/security/advisories/GHSA-q6r2-x2cc-vrp7>
- <https://github.com/git-ecosystem/git-credential-manager/security/advisories/GHSA-86c2-4x57-wc8g>
- <https://github.com/desktop/desktop/security/advisories/GHSA-36mm-rh9q-cpqq>
- <https://github.com/cli/cli/security/advisories/GHSA-jwcm-9g39-pmcw>
- <https://github.com/git/git/security/advisories/GHSA-r5ph-xg7q-xfrp>
- <https://github.com/git/git/security/advisories/GHSA-hmg8-h7qf-7cxr>