DevSecOps : GitLab 13.4 mêle CI et Vault

GitLab a annoncé cette semaine la disponibilité générale de GitLab 13.4, sa plateforme de développement et de gestion de dépôts de code source.

Avec la version 13.4, GitLab étend les capacités DevSecOps de la plateforme avec de nouvelles fonctionnalités, parmi lesquelles :

– l'injection directe dans les processus d'intégration continue (CI) des secrets* gérés dans le coffre-fort Vault de Hashicorp
– l'intégration du nouvel agent GitLab Kubernets (GKA)
– la prise en charge du contrôle de version automatique pour les nouveaux fichiers d'état Terraform
– un GitLab Security Center (ex-tableau de bord de sécurité des instances de GitLab) avec rapports et paramètres de vulnérabilité.

Autoriser les déploiements sans accès au code

GitLab 13.4 intègre d'autres améliorations, dont l'autorisation du déploiement sans accès au code, pour maintenir séparées les tâches de développement et de déploiement.

Il est possible désormais « d'autoriser les contributeurs non-codeurs à approuver les demandes de fusion (merge requests) pour le déploiement, et à déployer réellement le code, sans leur accorder également d'accès en tant que mainteneur », a précisé GitLab.

L'entreprise a proposé aux développeurs la mise à niveau 13.4.1 pour les éditions Community et Enterprise de sa plateforme, dans la foulée du lancement de la v13.4.

> *GitLab 13.4 released with Vault for CI variables, Kubernetes Agent, and Security Center... and we're bringing feature flags to Starter!https://t.co/gwPJnQEbMI*
>
> *— GitLab (@gitlab) September 22, 2020*

*clés de chiffrement, identifiants, certificats, etc.