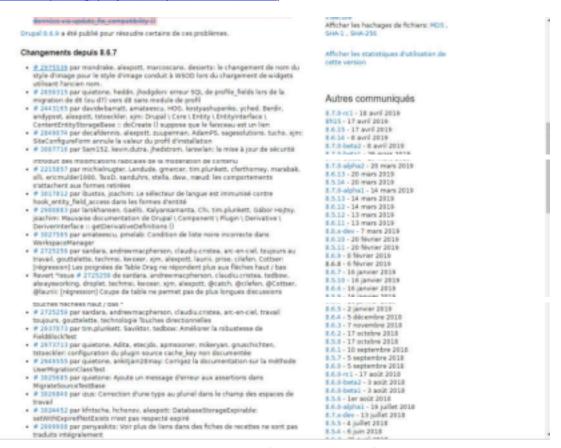
Ma veille technologique est portée sur le CMS DRUPAL.

Durant ma période de veille, Drupal à sorti 24 versions. La dernière version date du 28 septembre 2022 et est la version 9.4.7

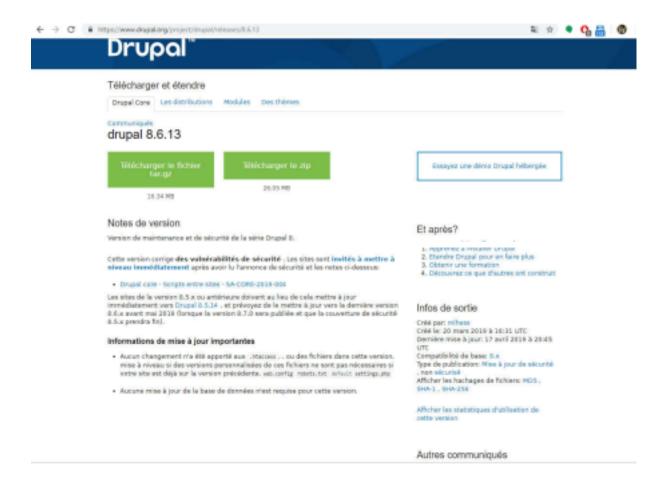
I EVOLUTION DU CMS A TRAVERS LES DIFFERENTES VERSIONS

Toutes ses versions ont pour but d'améliorer les performances du CMS, mais surtout d'augmenter sa fiabilité.

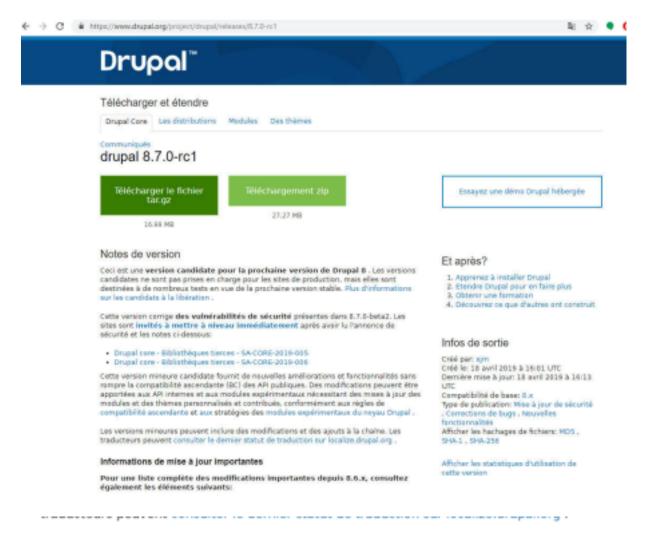
Nous pouvons voir la liste des versions de drupal sur le site de drupal (https://www.drupal.org/project/drupal/releases/8.6.8)



Toutes ces nouvelles versions apportent des mises à jour sur le système, par exemple, la version 8.6.13 améliore la sécurité du CMS par rapport à la version précédente (8.6.12). Comme vous pouvez le voir sur le site de drupal :



Ou encore, la dernière version de drupal sortie, est une version de test pour la prochaine version de drupal. Cette dernière version à résout les bugs et problèmes importants présents sur la version précédente :



Informations de mise à jour importantes

Pour une liste complète des modifications importantes depuis 8.6.x, consultez également les éléments suivants:

- Notes de publication de 8.7.0-alpha1
- Notes de publication de 8.7.0-alpha2
- Notes de publication de la version 8.7.0-beta1
- Notes de publication de la version 8.7.0-beta2.

Les personnes qui envisagent de mettre à jour cette version devraient prendre en compte les points importants suivants:

 Les opérations de schéma d'entité laisseront maintenant les tables de sauvegarde en place pour l'inspection. Voir l'enregistrement de modification sur les données de sauvegarde de la mise à jour de l'entité pour plus de détails, y compris sur la façon de désactiver cette fonctionnalité.

Correction de bugs importants

Les problèmes importants suivants sont résolus dans Drupal 8.7.0-rc1.

Problèmes résolus du programme de test bêta des versions mineures

À partir de Drupal 8.7.0-beta1, l'association Drupal et les principaux responsables de Drupal collaborent avec les agences et les propriétaires de site dans le cadre d'un programme de test bêta officiel des versions mineures de Drupal. Le programme vise à identifier et à minimiser les régressions dans les versions mineures. Participer au programme est un moyen de contribuer au projet Drupal et sera crédité en conséquence. Malgré une forte fiabilité, le cms à connu dès février 2019, des failles de sécurité dans son système. En effet, plusieurs articles parlent de faillent qui ont permis à des cybercriminels d'attaquer des sites conçus en Drupal grâce à des failles sur ce dernier.

Comme nous en parle l'article paru le 22 avril 2019 sur le site programmez.com



Des attaques cybercriminelles ont eu lieu notamment sur des sites de crypto-monnaie grâce à module qui permet de les extraire.

Comme nous en parle cet article de zdnet.com :



nouveau bug Drupal

Sécurité: Une vulnérabilité a été découverte et corrigée par le projet la semaine dernière. La publication du code d'exploitation a aidé les pirates informatiques à faire décoller les attaques de Drupal.



Trois jours - c'est le temps qu'il a fallu aux pirates pour lancer des attaques contre les sites Drupal en utilisant un exploit pour une faille de sécurité que le projet de CMS avait corrigée la semaine dernière.

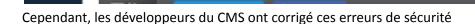


Les attaques, détectées par la société de pare-feu Web Imperva, ont tenté de tirer parti des sites Drupal qui n'avaient pas encore été mis à jour. L'objectif de ces attaques était de mettre en place un module de cryptojacking JavaScript, CoinIMP, sur des sites vulnérables.

Le script d'extraction de cryptomonnaie, qui fonctionne de la même manière que le célèbre module Coinhive, aurait utilisé les navigateurs des visiteurs du site pour extraire la cryptomonnaie Monero pour le compte des pirates.

Selon Imperva, les attaques ont commencé le samedi 23 février, trois jours après que le projet Drupal ait corrigé une vulnérabilité connue sous le nom de CVE-2019-6340, et deux jours après que le code d'exploitation de preuve de concept (PoC) ait été rendu largement disponible en ligne sur différents sites [1, 2].

Imperva explique que les centaines d'attaques détectées ont utilisé l'un des PoC comme base pour sa routine d'exploitation, prouvant une fois de plus que la publication d'un code de preuve de concept aide principalement les attaquants plutôt que les propriétaires de sites.





Source: https://www.nextinpact.com/brief/drupal-colmate-plusieurs-breches-importantes-de-securite-8494.htm.