

Synthese veille technologique

Ma veille technologique est portée sur le CMS DRUPAL.

Durant ma période de veille, Drupal a 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>)

The screenshot displays the Drupal 8.6.8 release page. At the top, it states "Drupal 8.6.8 a été publié pour résoudre certains de ces problèmes." Below this, a section titled "Changements depuis 8.6.7" lists numerous updates and bug fixes, including changes to the style system, migration of the profile field, and security updates. To the right, there are links to "Afficher les hachages de fichiers MD5, SHA-1, SHA-256" and "Afficher les statistiques d'utilisation de cette version". Below the main list of changes, a section titled "Autres communiqués" provides a timeline of previous releases from 8.6.3 to 8.6.8, including their dates and specific features or fixes.

Drupal 8.6.8 a été publié pour résoudre certains de ces problèmes.

Changements depuis 8.6.7

- # 2875535 par mandrake, alexpott, marroscano, deserts: le changement de nom du style d'image pour le style d'image conduit à un 500 lors du chargement de widgets utilisant l'ancien nom.
- # 2859335 par quetone, hedd, jhodgson: erreur SQL de profile_field lors de la migration de 48 (ou 47) vers 49 sans module de profil.
- # 2443065 par davidhamatt, amateescu, MOD, kostyashenko, yched, Berdr, andypost, alexpott, tstaackler, xjm: Drupal \Core \Entity \EntityInterface \ContentEntityStorageBase::create() suppose que le lanceur est un lien.
- # 2849874 par decalendis, alexpott, zupeman, AdamPS, sagesolutions, tuche, xjm: SiteConfigureForm annule la valeur du profil d'installation.
- # 3087728 par Sam152, KevinDubé, jhedstrom, laroclan: la mise à jour de sécurité introduit des modifications radicales de la modération de contenu.
- # 2215857 par michelrugier, Lendude, gmeier, timplunkett, clerthamey, marabak, olli, ericmulder1980, lisd, sanduhr, stella, davi, noxud: les comportements s'attachent aux formes résiliées.
- # 3017812 par ibutts, joachim: Le sélecteur de langue est immunisé contre hook_entity_field_access dans les formes d'entité.
- # 2960883 par lankhansen, Gaëlle, Kalyanamanta, Chi, timplunkett, Gábor Hejty, joachim: Mauvaise documentation de Drupal \Component \Plugin \Derivative \DerivativeInterface::getDerivativeDefinitions().
- # 3027595 par amateescu, prelate: Condition de liste noire incorrecte dans WorkspaceManager.
- # 2725259 par sandara, andrewmacpherson, claudiu.crotes, arc-en-ciel, toujours au travail, gouttelette, techmsi, kovser, xjm, alexpott, launi, prise, cilefen, Cottser [régression] Les poignées de Table Drag ne répondent plus aux flèches haut / bas.
- Revert l'issue # 2725259 de sandara, andrewmacpherson, claudiu.crotes, tedbow, alwaysworking, drisplet, techmsi, kovser, xjm, alexpott, @catch, @cilefen, @Cottser, @launi: [régression] Coupe de table ne permet pas de plus longues discussions touchées recrées haut / bas.
- # 2725259 par sandara, andrewmacpherson, claudiu.crotes, arc-en-ciel, travail toujours, gouttelette, technologie Touches directionnelles.
- # 2937872 par timplunkett, Saviktar, tedbow: Améliorer la robustesse de FieldBlockTest.
- # 2973722 par quetone, Adita, etecjdo, apmasoner, mikeryan, gouschichten, tstaackler: configuration du plugin source cache, key non documentée.
- # 2949555 par quetone, aniketan28may: Corrigé la documentation sur la méthode UserMigrationClassTest.
- # 3025485 par quetone: Ajoute un message d'erreur aux assertions dans MigrateSourceTestBase.
- # 3026848 par izus: Correction d'une typo au pluriel dans le champ des espaces de travail.
- # 3024452 par kfrtsche, hchenev, alexpott: DatabaseStorageExpirable::setWithExpiryNotExists n'est pas respecté expiré.
- # 2999988 par penysakito: Voir plus de liens dans des fiches de recettes ne sont pas traduits intégralement.

Autres communiqués

- 8.7.0-rc1 - 18 avril 2019
- 8.6.5 - 17 avril 2019
- 8.6.15 - 17 avril 2019
- 8.6.14 - 8 avril 2019
- 8.7.0-beta2 - 8 avril 2019
- 8.7.0-alpha2 - 29 mars 2019
- 8.6.13 - 20 mars 2019
- 8.6.14 - 20 mars 2019
- 8.7.0-alpha1 - 14 mars 2019
- 8.6.12 - 14 mars 2019
- 8.6.12 - 14 mars 2019
- 8.6.12 - 13 mars 2019
- 8.6.11 - 13 mars 2019
- 8.6.x-dev - 7 mars 2019
- 8.6.10 - 20 février 2019
- 8.6.11 - 20 février 2019
- 8.6.9 - 8 février 2019
- 8.6.8 - 6 février 2019
- 8.6.7 - 16 janvier 2019
- 8.6.10 - 16 janvier 2019
- 8.6.6 - 16 janvier 2019
- 8.6.5 - 10 janvier 2019
- 8.6.4 - 2 janvier 2019
- 8.6.3 - 5 décembre 2018
- 8.6.2 - 7 novembre 2018
- 8.6.2 - 17 octobre 2018
- 8.6.1 - 17 octobre 2018
- 8.6.1 - 10 septembre 2018
- 8.6.7 - 5 septembre 2018
- 8.6.8 - 5 septembre 2018
- 8.6.8-rc1 - 17 août 2018
- 8.6.8-beta2 - 3 août 2018
- 8.6.8-beta1 - 3 août 2018
- 8.6.6 - 1er août 2018
- 8.6.8-alpha1 - 19 juillet 2018
- 8.7.x-dev - 13 juillet 2018
- 8.6.5 - 4 juillet 2018
- 8.6.4 - 6 juin 2018

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 :

← → ↻ <https://www.drupal.org/project/drupal/releases/8.6.13> 🏠 ☆ 🔍 📄 📱

Drupal™

Télécharger et étendre

Drupal Core [Les distributions](#) [Modules](#) [Des thèmes](#)

Communiqués

drupal 8.6.13

Télécharger le fichier tar.gz
26.34 MB

Télécharger le zip
26.05 MB

Essayez une démo Drupal hébergée.

Notes de version

Version de maintenance et de sécurité de la série Drupal 8.

Cette version corrige **des vulnérabilités de sécurité**. Les sites sont **invités à mettre à niveau immédiatement** après avoir lu l'annonce de sécurité et les notes ci-dessous :

- Drupal core - scripts entre sites - SA-CORE-2019-004

Les sites de la version 8.5.x ou antérieure doivent au lieu de cela mettre à jour immédiatement vers [Drupal 8.5.14](#), et prévoir de le mettre à jour vers la dernière version 8.6.x avant mai 2019 (lorsque la version 8.7.0 sera publiée et que la couverture de sécurité 8.5.x prendra fin).

Informations de mise à jour importantes

- Aucun changement n'a été apporté aux `install.*` ou des fichiers dans cette version, mise à niveau si des versions personnalisées de ces fichiers ne sont pas nécessaires si votre site est déjà sur la version précédente. `web.config`, `robots.txt`, `default.settings.php`.
- Aucune mise à jour de la base de données n'est requise pour cette version.

Et après?

- Apprenez à installer Drupal
- Étendez Drupal pour en faire plus
- Obtenez une formation
- Découvrez ce que d'autres ont construit

Infos de sortie

Créé par: [mihess](#)
 Créé le: 20 mars 2019 à 16:31 UTC
 Dernière mise à jour: 17 avril 2019 à 20:45 UTC
 Compatibilité de base: 5.x
 Type de publication: Mise à jour de sécurité, non sécurisé
 Afficher les hachages de fichiers: MD5, SHA-1, SHA-256

[Afficher les statistiques d'utilisation de cette version](#)

Autres communiqués

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 :

← → ↻ <https://www.drupal.org/project/drupal/releases/8.7.0-rc1> 📄 ☆ 🌐

Drupal™

Télécharger et étendre

Drupal Core Les distributions Modules Des thèmes

Communiqués
drupal 8.7.0-rc1

Télécharger le fichier tar.gz
16.99 Mo

Téléchargement zip
27.27 Mo

Essayez une démo Drupal hébergée

Notes de version

Ceci est une **version candidate pour la prochaine version de Drupal 8**. Les versions candidates ne sont pas prises en charge pour les sites de production, mais elles sont destinées à de nombreux tests en vue de la prochaine version stable. [Plus d'informations sur les candidats à la libération](#).

Cette version corrige **des vulnérabilités de sécurité** présentes dans 8.7.0-beta2. Les sites sont **invités à mettre à niveau immédiatement** après avoir lu l'annonce de sécurité et les notes ci-dessous:

- [Drupal core - Bibliothèques tierces - SA-CORE-2019-035](#)
- [Drupal core - Bibliothèques tierces - SA-CORE-2019-036](#)

Cette version mineure candidate fournit de nouvelles améliorations et fonctionnalités sans rompre la compatibilité ascendante (BC) des API publiques. Des modifications peuvent être apportées aux API internes et aux modules expérimentaux nécessitant des mises à jour des modules et des thèmes personnalisés et contribués, conformément aux règles de [compatibilité ascendante](#) et aux stratégies des [modules expérimentaux du noyau Drupal](#).

Les versions mineures peuvent inclure des modifications et des ajouts à la chaîne. Les traducteurs peuvent consulter le dernier statut de traduction sur localize.drupal.org.

Et après?

1. Apprenez à installer Drupal
2. Étendre Drupal pour en faire plus
3. Obtenir une formation
4. Découvrez ce que d'autres ont construit

Infos de sortie

Créé par: xjm
Créé le: 18 avril 2019 à 16:01 UTC
Dernière mise à jour: 18 avril 2019 à 16:13 UTC
Compatibilité de base: 8.x
Type de publication: Mise à jour de sécurité, Corrections de bugs, Nouvelles fonctionnalités
Afficher les hachages de fichiers: MD5, SHA-1, SHA-256

[Afficher les statistiques d'utilisation de cette version](#)

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.

II DES FAILLES DE SECURITES DETECTEES

Malgré une forte fiabilité, le cms a connu dès février 2019, des failles de sécurité dans son système. En effet, plusieurs articles parlent de failles 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

Une vulnérabilité hautement critique découverte dans Drupal 8 et dans certains modules pour Drupal 7

Par: fredericmazue | ven, 22/02/2019 - 15:41

Drupal, faille, vulnérabilité

J'aime 1,5 K Partager 0 Tweeter Partager

Une vulnérabilité hautement critique a été découverte dans Drupal 8. Un défaut d'assainissement des données reçues par le célèbre CMS en dehors des formulaires induit cette vulnérabilité qui, si elle est exploitée, peut conduire à l'exécution de code PHP arbitraire à distance. Ceci lorsque le module 'Core' RESTful Web Services (rest) de Drupal 8 est activé, ou si un autre module de type Web Services (tel que JSON:API par exemple) est installé et activé.

Cette vulnérabilité concerne les branches 8.6.x et 8.5.x de Drupal 8 (Les versions antérieures, en fin de vie, ne reçoivent plus de correctifs de sécurité). La vulnérabilité est corrigée dans Drupal 8.6.10 et 8.5.11 respectivement.

L'équipe de développement de Drupal insiste sur l'urgence absolue qu'il y a à appliquer ces correctifs. Si cela n'est pas possible dans l'immédiat, les administrateurs peuvent désactiver tous les modules de types Web Service ou peuvent configurer leur serveur Web afin qu'il ne permette pas les requêtes PUT/PATCH/POST vers les ressources Web Services.

Une histoire de la micro-informatique : les ordinateurs de 1973 à 2007

Commodore 64, Oric, Osborne, Zorba, TRS-80, 70, 80 et 90 furent l'ordinateur. Ce mook (mini-livre) retrace cette histoire.

[Acheter](#)

Abonnements en vol

Nous proposons aux entrées des tarifs spéciaux équipes à partir de 5 personnes.

[En savoir plus](#)

Le cloud computing et les développeurs : Comment

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

Comme nous en parle cet article de zdnet.com :

0 Réactions

26 J'aime

Twitter

Partager

plus +

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.



Par Catalin Cimpanu | Modifié le mercredi 27 févr. 2019 à 11:44

Suivre @zdnnet

in Suivre

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.

Cependant, les développeurs du CMS ont corrigé ces erreurs de sécurité



Drupal colmate plusieurs brèches importantes de sécurité

Date ▼

Drupal a déployé des correctifs de sécurité pour colmater un lot de brèches jugées « modérément critiques ».

Toutes ces vulnérabilités se trouvent dans les bibliothèques tierces accompagnant les versions 8.7.6, 8.5 et même la 7.

L'une des plus importantes est de type XSS (cross-site scripting) et réside dans le plugin JQuery, toujours fourni avec Drupal Core. La faille en question avait été corrigée la semaine dernière lors de la publication de JQuery 3.4.0.

Les autres failles résident dans les composants Symfony PHP et pourraient entraîner des attaques de type XSS, une exécution de code arbitraire à distance ou un contournement de l'authentification.

Il est évidemment conseillé de mettre à jour les installations Drupal aussi rapidement que possible.



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