

Une IA a trouvé la faille qui menace 7 sites web sur 10

Bon vendredi à tous.

Mercredi, 2 failles graves découvertes avec l'aide de l'IA dans PHP, la technologie qui fait tourner 7 sites web sur 10, ont poussé la Finlande à couper une partie de ses sites publics. Si votre site tourne sous WordPress, la première actu vous concerne directement. Ensuite : Anthropic teste une IA qui surveille vos outils à votre place et dévoile ses comptes avant la Bourse, Meta inquiète Wall Street avec ses dépenses, et le français Mistral s'attaque à la voix. On termine avec Descript, un logiciel qui monte vos vidéos comme on corrige un texte.

Quelqu'un devrait lire ça ?

AU SOMMAIRE

- 01 Des IA ont trouvé une faille dans PHP, la technologie qui fait tourner 7 sites web sur 10
- 02 Anthropic teste Claude Duet, une IA qui surveille vos outils et vous prévient quand il faut agir
- 03 Anthropic a vendu pour 16,3 milliards de dollars en 6 mois, mais affiche 80,7 milliards de pertes
- 04 Meta va dépenser jusqu'à 145 milliards de dollars dans l'IA cette année, et la Bourse s'inquiète
- 05 Le français Mistral lance des IA vocales pour fabriquer des assistants qui répondent au téléphone



01

Des IA ont trouvé une faille dans PHP, la technologie qui fait tourner 7 sites web sur 10

Mercredi, des sites publics ont été coupés en urgence en Europe. En cause, 2 failles graves découvertes avec l'aide de l'IA dans PHP, le langage sur lequel repose WordPress.

PHP est un langage informatique (la technologie qui fabrique les pages d'un site au moment où vous les ouvrez). Il fait tourner environ 70 % des sites web, dont ceux construits avec WordPress, Drupal ou Joomla. Les 2 failles, baptisées PHP2Shell, permettent à un pirate de prendre le contrôle d'un serveur à distance, sans aucun mot de passe. Presque toutes les versions de PHP publiées depuis 10 ans sont concernées.

Elles ont été trouvées avec l'aide de l'IA. L'entreprise de cybersécurité Wiz s'est servie de Gemini et de GPT-5.6 Sol, un modèle d'OpenAI, pour repérer les bugs puis fabriquer en quelques heures des attaques qui fonctionnent sur WordPress. Wiz a prévenu l'équipe de PHP le 24 août et le correctif est sorti mercredi 21 octobre. Le jour même, la Finlande a coupé une partie de ses sites publics par précaution, et Amazon Web Services signalait déjà des attaques en cours.

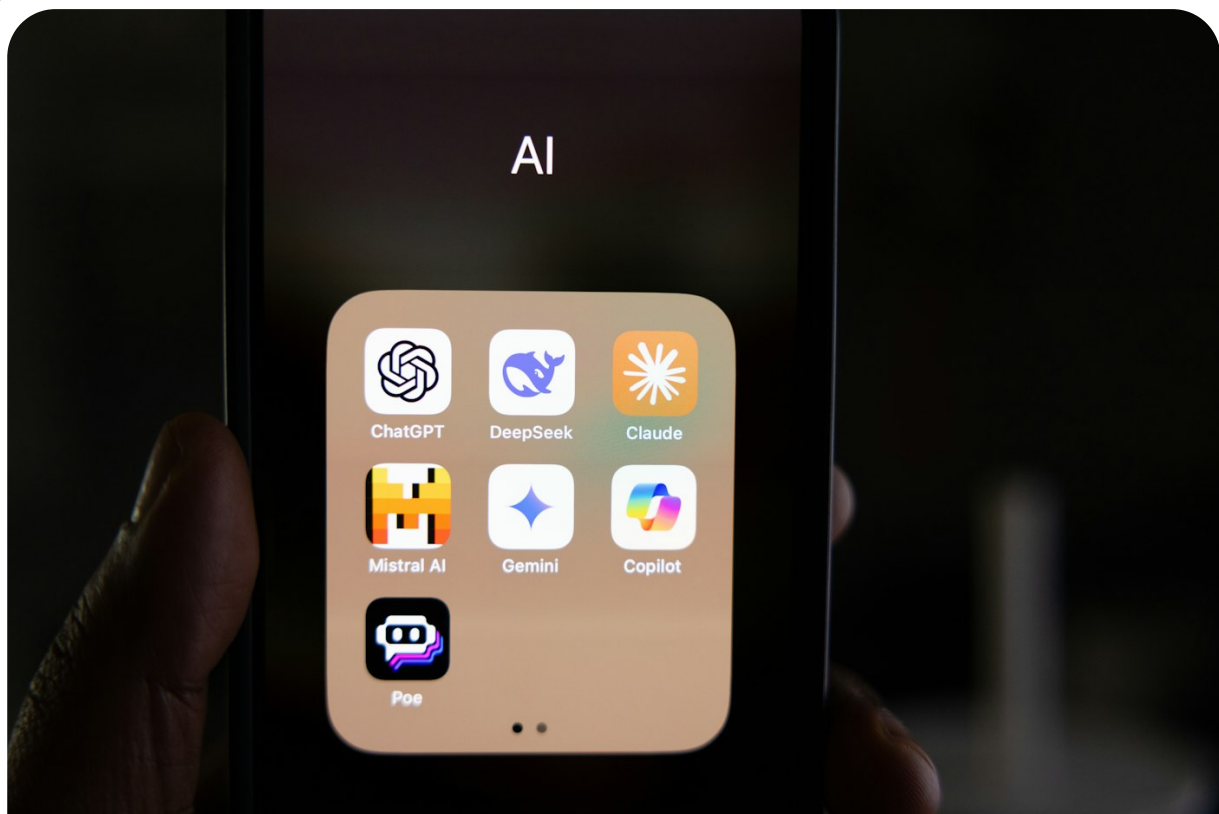
Les experts redoutent la suite : ce que l'IA a permis aux chercheurs, elle le permettra bientôt aux pirates. Pour un entrepreneur, la consigne est simple et urgente. Si votre site tourne sous WordPress ou une autre solution en PHP, demandez dès aujourd'hui à votre hébergeur ou à votre prestataire si la mise à jour de PHP est faite. C'est souvent l'hébergeur qui s'en charge, mais mieux vaut le vérifier que le supposer.

Le regard KLEAA

Cette affaire montre que le délai entre la découverte d'une faille et son exploitation se compte désormais en jours, pas en mois. Les plus exposés ne sont pas les grands groupes, qui ont des équipes de sécurité, mais les petites structures : un site vitrine installé il y a 5 ans par un freelance et jamais mis à jour est exactement la cible facile. Si vous ne savez pas qui s'occupe de la maintenance de votre site, c'est le moment de le découvrir, et de prévoir un contrat de mise à jour plutôt qu'une intervention en urgence à chaque alerte.



Auguste Freton
Rédacteur KLEAA



02

Anthropic teste Claude Duet, une IA qui surveille vos outils et vous prévient quand il faut agir

Au lieu d'attendre vos questions, Duet parcourt vos messageries et vos logiciels, vous envoie un point chaque matin et avance sur des tâches pendant que vous faites autre chose.

Anthropic, le créateur de Claude, a présenté mercredi 21 octobre Claude Duet, un agent IA (un logiciel qui agit seul pour accomplir une mission) pensé pour les professionnels et les dirigeants de petites entreprises. Chaque matin, il envoie un résumé court de ce qui compte dans vos applications connectées. Il les vérifie ensuite toutes les quelques heures et ne vous écrit que si quelque chose demande votre attention.

Vous pouvez aussi lui confier des tâches : caler une réunion, préparer un tableau de bord, une prévision de ventes ou même une petite application web. Il travaille sur son propre ordinateur virtuel (une machine louée dans le cloud), donc votre téléphone peut rester éteint. Duet se branche sur plus de 6 000 services, dont Gmail, Slack, Stripe, HubSpot, Shopify ou QuickBooks. Chez les premiers testeurs, il a par exemple regroupé les factures de 110 points de vente ou proposé de déplacer un appel qui tombait pendant un vol.

Garde-fou annoncé : Duet demande votre accord avant d'envoyer un message, de payer, de signer ou de supprimer quoi que ce soit, et certaines actions, comme déplacer de l'argent entre comptes, lui restent interdites. Pour l'instant, il n'est ouvert que sur liste d'attente, aux abonnés Pro et Max aux États-Unis, sans surcoût. Anthropic reconnaît qu'il peut encore mal lire une conversation ou se tromper sur l'urgence. La promesse, pour une petite équipe : un assistant qui trie à votre place ce qui mérite votre temps.

Le regard KLEAA

Laisser une IA lire votre messagerie, votre comptabilité et vos ventes, c'est lui confier les clés de la maison. L'intérêt est réel pour une équipe de 3 personnes sans assistant. Mais quand Duet arrivera en France, commencez petit : 1 ou 2 outils connectés, jamais la banque, et une semaine à vérifier ses alertes avant de lui faire confiance. Une IA qui se trompe sur l'urgence vous fait perdre 5 minutes. Une IA qui se trompe en écrivant à un client peut vous faire perdre le client.



Auguste Freton
Rédacteur KLEAA



03

Anthropic a vendu pour 16,3 milliards de dollars en 6 mois, mais affiche 80,7 milliards de pertes

Le document préparé pour l'entrée en Bourse du créateur de Claude dévoile ses comptes. Les ventes s'envolent, la facture de puissance de calcul aussi.

Pour entrer en Bourse, une entreprise doit publier un prospectus (le document qui détaille ses comptes et ses risques aux futurs actionnaires). Celui d'Anthropic, encore à l'état de brouillon, a été consulté par le Wall Street Journal. Il montre 16,3 milliards de dollars de chiffre d'affaires au premier semestre 2026, porté par les entreprises qui paient pour Claude et Claude Code.

La perte affichée, 80,7 milliards de dollars, impressionne, mais environ 72 milliards viennent d'écritures comptables liées à la valeur de ses financements, pas d'argent réellement sorti des caisses. Le vrai poste lourd est ailleurs : près de 9 milliards de dollars dépensés en puissance de calcul en 6 mois, plus que les 7,3 milliards de toute l'année 2025. Anthropic s'est engagé pour plus de 600 milliards de dollars d'infrastructures dans les années à venir et prévient que le manque de puces pourrait freiner sa croissance.

Autre détail : environ 20 % des ventes viennent de 2 clients seulement. L'entrée en Bourse pourrait avoir lieu dès novembre. Pour les entreprises qui utilisent Claude, ces chiffres rassurent sur la solidité de la demande, mais rappellent que le prix de l'IA dépend d'abord du coût des machines. Tant que ce coût grimpe, rien ne garantit que les abonnements resteront au tarif actuel.



04

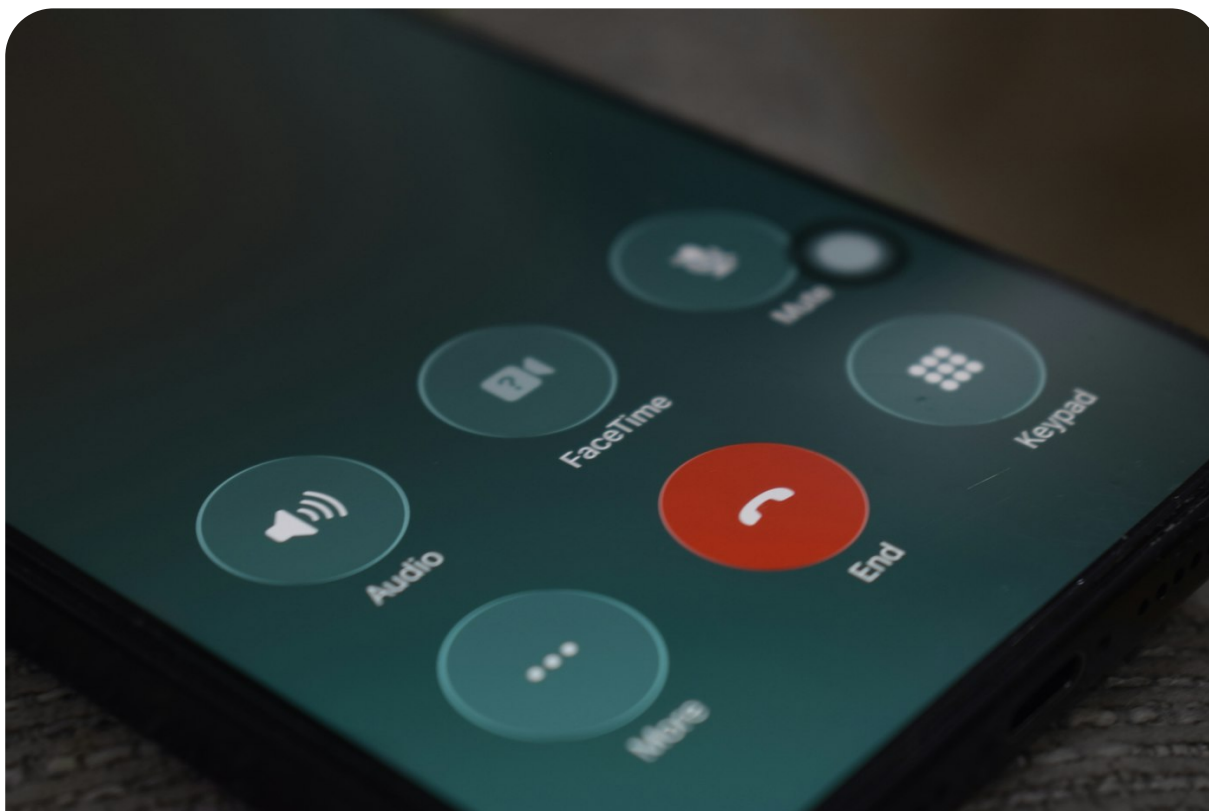
Meta va dépenser jusqu'à 145 milliards de dollars dans l'IA cette année, et la Bourse s'inquiète

Le propriétaire de Facebook, Instagram et WhatsApp a pourtant publié de bons résultats. Mais jeudi, son action perdait près de 6 % en séance, car l'IA engloutit l'argent qu'il gagne.

Mercredi soir, Meta a annoncé 64,6 milliards de dollars de chiffre d'affaires sur 3 mois, mieux que les 63,4 milliards attendus par les analystes. Mais il a aussi relevé ses dépenses d'investissement (l'argent mis dans les centres de données, les puces et les bâtiments) : entre 135 et 145 milliards de dollars cette année, contre 130 à 145 milliards annoncés jusqu'ici.

Conséquence : le flux de trésorerie disponible (l'argent qui reste une fois toutes les dépenses payées) est passé dans le rouge, à moins 2,1 milliards de dollars, contre plus 10,6 milliards un an plus tôt. Meta prévoit aussi de créer une nouvelle catégorie d'actions sans droit de vote, qui pourrait financer des rachats sans réduire le contrôle de Mark Zuckerberg.

C'est le paradoxe de l'IA en ce moment : les géants gagnent beaucoup d'argent, mais le dépensent encore plus vite pour ne pas se faire distancer. Et Meta gagne l'essentiel de son argent grâce à la publicité. Il a donc toutes les raisons de pousser ses outils publicitaires à base d'IA pour rentabiliser ces milliards. Attendez-vous à voir de plus en plus de réglages automatiques dans vos campagnes Facebook et Instagram.



05

Le français Mistral lance des IA vocales pour fabriquer des assistants qui répondent au téléphone

Voxtral 3 transcrit la parole dans plus de 50 langues et répond avec une voix de synthèse en moins d'une demi-seconde. Il peut aussi tourner sur les serveurs d'une entreprise.

Mistral AI, la start-up parisienne de l'IA, a dévoilé mardi 20 octobre Voxtral 3, une famille de modèles pour la voix. 3 modèles transforment la parole en texte, dont 1 en temps réel, et un 4e fait l'inverse : il lit un texte à voix haute. L'ensemble est livré avec une boîte à outils pour développeurs qui enchaîne l'écoute, la réflexion, l'action et la réponse parlée.

Concrètement, une entreprise peut s'en servir pour fabriquer un agent vocal (une IA qui tient une conversation au téléphone) : il comprend l'appelant, distingue qui parle, consulte un logiciel puis répond. Le modèle temps réel réagit en moins de 500 millisecondes, assez vite pour une conversation naturelle. La transcription couvre plus de 50 langues, la voix de synthèse plus de 35, et l'outil sait cloner une voix et se brancher sur une ligne téléphonique.

Côté prix, la transcription coûte 0,0035 dollar la minute en différé et 0,008 dollar en direct : une heure de réunion transcrite revient à environ 21 centimes de dollar. Atout pour les entreprises européennes : Voxtral 3 peut être utilisé depuis des serveurs situés en Europe, ou installé sur ses propres machines, sans envoyer les conversations de ses clients aux États-Unis. Pour un cabinet, une agence ou un service client, c'est une brique française pour automatiser l'accueil téléphonique sans dépendre des géants américains.

L'OUTIL

Descript

Descript (San Francisco) · Freemium · montage vidéo et podcast · Mac, Windows et navigateur

Descript transforme votre vidéo ou votre podcast en texte, et vous la montez en modifiant ce texte : supprimez une phrase, elle disparaît de la vidéo.

TARIF

Freemium. La version gratuite, sans carte bancaire, permet de traiter 1 heure d'enregistrement par mois, avec la transcription en français, les sous-titres animés et un essai des outils IA (100 crédits, une seule fois). Les vidéos s'exportent en 720p.

Ensuite : Hobbyist à 16 dollars par mois en facturation annuelle (24 dollars au mois), pour 10 heures par mois et des exports en 1080p sans filigrane. Creator, à 24 dollars par mois en annuel (35 dollars au mois), monte à 30 heures et à la 4K.

À quoi ça sert : monter une vidéo demande d'habitude un logiciel compliqué et des heures passées à couper sur une ligne de temps. Descript affiche chaque mot prononcé comme dans un document : quand vous effacez un mot, l'image et le son sont coupés au même endroit. En un clic, il retire les « euh », les silences et les prises ratées, nettoie la voix enregistrée dans une pièce bruyante et ajoute des sous-titres. Idéal pour une vidéo de présentation, un tutoriel pour vos clients, un webinaire ou un podcast.

Comment l'utiliser : 1) allez sur descript.com, créez un compte gratuit, puis installez l'application ou restez dans le navigateur (l'interface est en anglais) ; 2) créez un projet et importez votre vidéo, ou enregistrez-vous directement avec la webcam ou l'écran ; 3) attendez la transcription automatique, puis supprimez les passages inutiles dans le texte, comme dans un traitement de texte ; 4) cliquez sur « Remove Filler Words » pour enlever les hésitations et sur « Studio Sound » pour améliorer la voix ; 5) ajoutez les sous-titres, puis exportez la vidéo ou partagez-la par un lien.

Cas PME : une gérante d'agence immobilière filme au téléphone, en 15 minutes, la visite commentée d'un appartement. Dans Descript, elle efface ses hésitations et le passage où elle s'est trompée de surface, nettoie le bruit de la rue et ajoute des sous-titres pour ceux qui regardent sans le son. Une heure plus tard, la vidéo accompagne l'annonce et part sur ses réseaux, sans passer par un monteur.

À NE PAS CONFONDRE

Descript n'est pas Opus Clip, présenté ici en septembre : Opus Clip découpe automatiquement une longue vidéo en extraits courts, Descript sert à monter et à corriger la vidéo elle-même. Et sa fonction de voix clonée ne s'utilise que sur votre propre voix, ou avec l'accord écrit de la personne concernée.