Navigation
Inscrivez-vous gratuitement
pour pouvoir participer, suivre les réponses en temps réel, voter pour les messages, poser vos propres questions et recevoir la newsletter
JE M'INSCRIS

Discussion :
L'IA détecte les failles logicielles plus rapidement que Microsoft ne parvienne à les corriger
Sujet : *Intelligence artificielle*

30/07/2026, 15h36 #1

Mathis Lucas
Chroniqueur Actualités
Rédacteur technique
Inscrit en: Juin 2023
Messages: 2 000

L'IA détecte les failles logicielles plus rapidement que Microsoft ne parvienne à les corriger

Apocalypse des bogues : l'IA détecte les failles logicielles plus rapidement que les équipes de sécurité de Microsoft ne parviennent à les corriger

la dette technique du code hérité suscite des inquiétudes

Microsoft serait en proie à une crise informatique provoquée par la puissance inédite du modèle d'IA Claude Mythos d'Anthropic. Cet outil parvient à identifier des failles de sécurité à une cadence telle que les ingénieurs de Microsoft sont incapables de les corriger assez rapidement. Microsoft mène une course contre la montre pour sécuriser des logiciels mondiaux comme SharePoint avant que des attaquants n'exploitent ces mêmes failles. La stratégie habituelle de triage des bogues est remise en question, car l'IA permet désormais de combiner plusieurs failles mineures pour lancer des attaques dévastatrices. Les dirigeants craignent une apocalypse de bogues.

Claude Mythos est un nouveau modèle d'IA développé par Anthropic et doté de capacités avancées en matière de cybersécurité. Le géant de la technologie Microsoft a obtenu un accès privilégié à Mythos dans le cadre d'un programme baptisé Project Glasswing, une initiative de cybersécurité défensive lancée par Anthropic le 7 avril 2026. Mythos a été utilisé en interne pour analyser et détecter les failles de sécurité au sein des logiciels de Microsoft.

L'objectif était de détecter et de corriger ces vulnérabilités avant que des pirates informatiques et des gouvernements hostiles, comme celui de la Chine ou de la Russie, ne e les exploitent à leur tour à des fins d'espionnage et de sabotage. La version utilisée par Microsoft est baptisée « Claude Mythos Preview ».

D'autres entreprises telles que Mozilla, Amazon, et Apple participent également au programme Project Glasswing d'Anthropic. En avril, Mozilla a rapporté que Mythos avait détecté 271 failles de sécurité dans Firefox 150. Mozilla a expliqué que ce nouveau modèle d'IA est « tout aussi performant » que les meilleurs chercheurs en sécurité au monde. Selon l'entreprise, Mythos analyse le code source et identifie les bogues avec une « expertise pointue ».

Une course contre la montre face aux menaces cybernétiques

Selon un nouveau rapport publié de ProPublica, Mythos révélait des bogues plus rapidement que le géant technologique ne parvenait à les corriger. Un responsable a déclaré que les ingénieurs sont engagés dans une « course effrénée » pour combler ce retard. Lors d'une réunion interne à la mi-mai, une diapositive de la présentation montrait que rien qu'en avril, Mythos avait découvert 90 bogues « critiques » et 141 « importants » dans SharePoint.

AI Is Finding Your Vulnerabilities Faster Than You
TFiR

Watch on

Au cours de la première quinzaine de mai, il en a détecté encore davantage. Pour rappel, SharePoint est une plateforme collaborative conçue pour les organisations. Elle sert d'espace centralisé pour stocker, partager et gérer des documents. Elle permet également de créer des sites Web internes (intranet) pour communiquer et travailler en équipes sur différents projets. SharePoint est très répandu dans les grandes entreprises et administrations.

La pression était immense, car les dirigeants avaient identifié la date du 31 mai comme le moment où le reste du monde aurait potentiellement accès à des technologies équivalentes à Mythos. « S'il vous plaît, s'il vous plaît, s'il vous plaît, si votre organisation présente des bogues datant d'avril, corrigez-les », a imploré Hans Andersen, responsable de l'ingénierie, lors de la réunion. Ils disposaient de deux semaines pour tirer le meilleur parti de l'outil.

Les ingénieurs présents à la réunion ont remis en question cette affirmation, l'un d'entre eux résumant ainsi la situation : « en gros, vous estimez donc que si le logiciel est publié le 1er juin, les adversaires disposeront de nos failles dès le 2 juin ? » « Oui », a répondu une personne. « Oui », a renchéri une autre.

Une avalanche de vulnérabilités révélées en très peu de temps

Les chiffres publiés par Microsoft en juillet 2026 ne sont pas une erreur de frappe. Le Patch Tuesday de juillet chiffre le problème : 622 vulnérabilités en un mois. Microsoft a corrigé 622 bogues lors de sa mise à jour du Patch Tuesday du 14 juillet dernier, soit plus du triple du précédent record de juin, qui était de 206. C'est une forme étrange de progrès. Les bogues sont détectés plus rapidement. La liste des correctifs à appliquer s'allonge également.

La liste publiée en juillet comprend 416 failles Windows, 82 failles Office, 46 failles Microsoft Edge et 63 vulnérabilités classées comme critiques. Deux failles étaient déjà exploitées : CVE-2026-56155 dans Active Directory Federation Services et CVE-2026-56164 dans SharePoint Server. Il ne s'agit pas de systèmes obscurs situés à la périphérie de l'entreprise. L'un gère les identifiants de connexion. L'autre logiciel héberge les documents d'entreprise.

Outre le système d'IA Claude Mythos d'Anthropic, Microsoft utilise également son outil d'analyse multimodèle MDASH pour accélérer la détection de bogues. C'est là le véritable enjeu. L'IA ne se contente pas de produire davantage de logiciels. Elle modifie la cadence à laquelle les anciens logiciels sont inspectés.

La preuve la plus flagrante nous vient de Pékin. Bloomberg a rapporté en avril que le groupe « 360 Digital Security », également connu sous le nom de Qihoo 360, avait développé un agent de détection des vulnérabilités) basé sur l'IA qui a permis de découvrir près de 1 000 failles jusque-là inconnues, notamment dans Microsoft Office et OpenClaw, un framework open source destiné à la création et au déploiement rapide de workflows d'agents IA.

La stratégie de triage et le danger des vulnérabilités mineures

Confronté à ce déluge de bogues, la firme de Redmond doit trouver le moyen de les corriger rapidement afin d'éviter une exploitation massive aux conséquences désastreuses. Microsoft a dû prioriser ses efforts de correction. L'entreprise a choisi de traiter en urgence les failles critiques et importantes, qui sont les plus susceptibles de causer des dommages notables, tout en laissant temporairement de côté les bogues de gravité faible ou modérée.

Toutefois, cette stratégie de triage traditionnelle comporte des risques majeurs face aux capacités de l'IA. Vinh Nguyen, ancien spécialiste de l'IA pour l'Agence de sécurité nationale américaine (NSA), a averti que Mythos a la capacité de lier plusieurs petites failles entre elles pour orchestrer des attaques dévastatrices.

Pour souligner cette nouvelle menace, il a expliqué : « le problème maintenant, c'est que vous pouvez enchaîner quatre failles de bas niveau, et cela peut équivaloir à une gravité élevée ». De son côté, Microsoft défend sa méthode en affirmant que cette technique d'enchaînement de failles fait depuis longtemps partie de son évaluation des risques. Selon les experts, les entreprises devront reconsidérer leur approche en matière de triage.

Mythos, par exemple, est capable d'enchaîner une série de failles qui se renforcent mutuellement, ce qui signifie que les failles de gravité faible ou modérée qui ne sont pas corrigées pourraient ouvrir la voie à des attaques dévastatrices. « Si vous êtes Microsoft, la stratégie de triage actuelle risque de sous-estimer les risques », estime Vinh Nguyen. Microsoft a déclaré que « le volume global de bogues ne se stabilisera pas avant un certain temps ».

OpenAI suit les traces d'Anthropic dans la détection de bogues

OpenAI aborde ce même problème sous l'angle défensif. Le 6 mars, OpenAI a présenté « Codex Security sous forme d'aperçu de recherche destiné aux utilisateurs de ChatGPT Pro, Enterprise, Business et Edu. L'entreprise dirigée par Sam Altman a indiqué que le logiciel avait analysé plus de 1,2 million de commits dans des dépôts externes au cours de sa phase bêta et identifié 792 failles critiques et 10 561 vulnérabilités à haut niveau de gravité.

Le principe est simple : Codex Security établit le contexte d'une base de code, détecte les vulnérabilités potentielles, les valide dans un bac à sable et propose des correctifs. La différence n'est pas négligeable. Les scanners traditionnels génèrent déjà beaucoup de « bruit ». Or, les équipes de sécurité sont déjà submergées par ce bruit. Ce dont elles ont besoin, ce sont des résultats accompagnés de preuves et d'une feuille de route pour la correction.

OpenAI a ensuite déclaré en juin que Codex Security avait analysé plus de 30 millions de commits sur plus de 30 000 bases de code depuis la présentation préliminaire de la recherche en mars, et que les réviseurs avaient manuellement marqué plus de 70 000 résultats comme corrigés. Telle est désormais l'ampleur du travail. Il est impossible de tout examiner à la main. Il faut que des machines avancées aident les humains à déterminer ce qui est réel.

« Plutôt que de mettre de côté ce qui est aujourd'hui considéré comme des failles à faible risque, les entreprises devraient affecter du personnel au développement et au test de correctifs pour l'ensemble des vulnérabilités », a déclaré Vinh Nguyen. Les urgences informatiques ont besoin de davantage d'experts pour traiter aussi bien les failles mettant les systèmes en danger que les brèches mineures susceptibles de devenir « fatales » par la suite.

La dette technique insondable et « l'apocalypse des bogues »

Cette crise de sécurité met en lumière des problèmes systémiques plus profonds au sein de Microsoft et de l'industrie logicielle en général. Le code de nombreux produits Microsoft est ancien et accumule ce que l'on appelle une dette technique, rendant les logiciels particulièrement vulnérables aux nouvelles méthodes d'analyse de l'IA. Les experts en cybersécurité s'attendent à ce que l'IA accélère davantage la découverte de nouvelles vulnérabilités.

Historiquement, les équipes de sécurité de Microsoft ont souvent souffert d'un manque d'effectifs. D'après certains témoignages, la sécurité serait perçue en interne comme un centre de coûts, par opposition au développement de nouveaux produits, que les dirigeants de Microsoft considèrent comme un centre de profits.

Les utilisateurs de Microsoft pourraient être particulièrement vulnérables. La popularité de ses applications, utilisées dans le monde entier, en fait une cible fréquente et lucrative pour les pirates informatiques. Ben Edwards, un scientifique des données spécialisé dans la gestion des vulnérabilités logicielles, rappelle que le secteur des logiciels devait déjà faire face à un « volume intense avant même l'essor de l'IA ». L'IA accélère encore plus la cadence.

« Avant, c'était comme boire à un tuyau d'arrosage réglé sur jet puissant ; aujourd'hui, c'est comme boire à une lance à incendie. Ils disposaient peut-être d'équipes capables de gérer ce tuyau d'arrosage. Quant à savoir s'ils peuvent gérer la lance à incendie, c'est une autre histoire », a expliqué Ben Edwards.

Le « vibe coding » pose également un problème de sécurité

Le « vibe coding » désigne une façon de programmer où on laisse l'IA générative écrire le code à partir de simples descriptions en langage naturel, sans relire ni vraiment comprendre chaque ligne produite. On avance par essais-erreurs, en jugeant le résultat au "ressenti" (vibe) plutôt que par une analyse technique rigoureuse. Le terme a été popularisé par Andrej Karpathy, un informaticien slovaco-canadien qui a travaillé sur l'Autopilot de Tesla.

C'est ce qui explique l'inquiétude actuelle : le vibe coding accélère le développement, mais peut aussi multiplier les bogues et les failles de sécurité, puisque personne ne maîtrise réellement le code qui a été écrit. Mais encore, les chercheurs ont découvert que les vulnérabilités générées par le vibe coding n'ont rien de mystérieux. Elles ressemblent aux erreurs que les équipes pressées par le temps ont toujours commises, mais à un rythme plus soutenu.

Cloud Security Alliance a indiqué dans son rapport « AI Velocity Gap » que le nombre d'entrées CVE directement attribuables à du code généré par l'IA est passé de 6 en janvier à 35 en mars 2026. Dans sa note de recherche d'avril 2026, Cloud Security Alliance a mis en évidence les secrets codés en dur par les outils d'IA de codage, les failles d'injection et les paramètres par défaut non sécurisés comme des catégories courantes de défaillances.

Pour une startup, cela change la donne. Cursor, Claude Code, Codex et d'autres outils similaires peuvent aider à livrer du code fonctionnel bien plus rapidement qu'une petite équipe ne pourrait le faire seule. Cependant, ils n'offrent pas pour autant une fonction de sécurité gratuite. Ce n'est pas un argument contre l'utilisation d'outils de codage basés sur l'IA. La bonne question est de savoir si votre cycle de révision a rattrapé votre cycle de compilation.

Windows perd du terrain au profit des distributions Linux

Windows 11 accumule les reproches depuis son lancement : interface remaniée au détriment de l'ergonomie, menu Démarrer jugé régressif, mises à jour intempestives qui ralentissent ou déstabilisent les machines, et une intégration forcée de Copilot que beaucoup vivent comme une intrusion. Copilot s'invite en effet partout sans vraiment se rendre utile, consommant des ressources et brouillant une expérience utilisateur déjà fragile.

Les ennuis sont bien documentés et concrets. Depuis juillet 2025, la mise à jour 24H2 (KB5062553) a introduit des bogues majeurs liés aux composants XAML : menu Démarrer qui refuse de s'ouvrir, barre des tâches qui disparaît, explorateur de fichiers instable, écran noir à la connexion, etc. Microsoft a mis quatre mois à reconnaître publiquement le problème. Plus de 5 ans après son lancement, Windows 11 est loin d'être un système stable.

Et ce n'était pas fini : après le Patch Tuesday de janvier 2026, de nombreux utilisateurs ont signalé que leurs PC se retrouvaient incapables de s'éteindre, coincés dans des cycles de redémarrage infinis. Microsoft a dû publier six mises à jour d'urgence hors de son calendrier habituel pour colmater les brèches. En raison des dérives de Microsoft, Windows a commencé à perdre du terrain face aux distributions Linux de plus en plus conviviales.

Les données de StatCounter pour juin 2026 indiquent que Windows représentait 56,55 % de l'utilisation mondiale des systèmes d'exploitation pour ordinateurs de bureau, ce qui a fait passer la part de marché de Microsoft sous la barre des 60 % pour la première fois depuis des années. Linux, quant à lui, a atteint 4,39 %, l'une de ses meilleures performances de tous les temps. Ces chiffrent tombent dans un contexte de rejet massif de Windows 11.

Et vous ?

➡ Quel est votre avis sur le sujet ?
➡ Que pensez-vous de la vitesse à laquelle l'IA découvre de nouvelles failles de sécurité ?
➡ Comment l'industrie technologique peut-elle faire face à cette nouvelle cadence imposée par l'IA ?
➡ L'IA pourrait permettre de combiner plusieurs failles mineures pour mener des attaques dévastatrices. Qu'en pensez-vous ?
➡ Les équipes de Microsoft sont submergées par l'avalanche de vulnérabilités révélées par l'IA. Quels sont les risques pour les utilisateurs ?

Voir aussi

➡ Satya Nadella veut recentrer Microsoft sur la qualité technique et la sécurité. Il nomme un nouveau tsar de la qualité de l'ingénierie, après le désastre des dernières mises à jour de Windows 11

➡ Les administrateurs informatiques en ont « ras-le-bol » des applications et produits « inutiles » de Microsoft et de Windows 11, tandis que Microsoft est occupé à intégrer Copilot dans chaque recoin de l'OS

Mythos d'Anthropic a détecté 271 failles de sécurité dans Mozilla Firefox 150, Mozilla affirme que ce nouveau modèle d'IA est « tout aussi performant » que les meilleurs chercheurs en sécurité au monde

Répondre avec citation | 30 | 0

30/07/2026, 20h53 #2

Matthieu Vergne

Membre éprouvé

Consultant IT, chercheur IA indépendant
Inscrit en: Novembre 2011
Messages: 2 492
Billets dans le blog: 3

> Envoyé par **Mathis Lucas**
>
> ***Apocalypse des bogues : l'IA détecte les failles logicielles plus rapidement que les équipes de sécurité de Microsoft ne parviennent à les corriger***

Remplacez "l'IA" par "les utilisateurs", ça marche aussi... Et ça fait des décennies que c'est vrai. Rien de nouveau sous le soleil (si ce n'est ses fortes températures).

Site perso
Recommandations pour débattre sainement

Références récurrentes :
The Cambridge Handbook of Expertise and Expert Performance
L'Art d'avoir toujours raison (ou ce qu'il faut éviter pour pas que je vous saute à la gorge {^_^})

Répondre avec citation | 4 | 0

Hier, 08h48 #3

Anselme45

Membre extrêmement actif

Développeur informatique
Inscrit en: Octobre 2017
Messages: 2 957

> Envoyé par **Matthieu Vergne**
>
> *Remplacez "l'IA" par "les utilisateurs", ça marche aussi... Et ça fait des décennies que c'est vrai. Rien de nouveau sous le soleil (si ce n'est ses fortes températures).*

Oh... Il y a bien longtemps que microsoft ne sait plus ce que c'est un "utilisateur"!!!

S'il arrivait aux "génies" de microsoft de croiser de temps à autre un "utilisateur", il n'aurait pas mis en oeuvre ne serait-ce que 10% des fonctionnalités inutiles qu'ils ne cessent d'ajouter à win11

Répondre avec citation | 2 | 0

Hier, 08h57 #4

Anselme45

Membre extrêmement actif

> *Apocalypse des bogues : l'IA détecte les failles logicielles plus rapidement que les équipes de sécurité de Microsoft ne parviennent à les corriger*
> *la dette technique du code hérité suscite des inquiétudes*

Développeur informatique
Inscrit en: Octobre 2017
Messages: 2 957

Mais comment? microsoft ne fait pas corriger ses bugs par des agents IA bien plus efficaces et plus productifs que ces "équipes de sécurité" d'un autre temps composés d'humains poussifs incapables de suivre la cadence??????????????????????

Répondre avec citation | 3 | 0

Hier, 14h04 #5

Fagus
Membre éprouvé
programmeur du dimanche
Inscrit en: Novembre 2003
Messages: 1 172

On rigole parce que c'est Microsoft et vendredi, mais la situation est probablement similaire ailleurs.
On parle beaucoup de mythos, mais GLM aurait des capacités en cybersécurité voisines. Et encore, c'est juste un modèle ouvert que les Chinois veulent bien donner (ils ont arrêté de publier certaines avancées).
Quid des autres OS et logiciels ? N'importe quel groupe de hackers avec un peu d'argent peut faire tourner GLM.

Répondre avec citation | 0 | 0

+ Répondre à la discussion   Signaler un problème

Forum   Général Développement   Algorithme & Mathématiques   Intelligence artificielle
L'IA détecte les failles logicielles plus rapidement que Microsoft ne parvienne à les corriger

« Discussion précédente | Discussion suivante »

Discussions similaires

Les ingénieurs d'IBM produisent une puce sur graphème 10 000 fois plus rapide que les précédentes
Par ToTo13 dans le forum Algorithmes et structures de données
Réponses: 0
Dernier message: 08/02/2014, 06h01

Les attaques DDoS plus larges et plus rapides que jamais
Par Stéphane le calme dans le forum Sécurité
Réponses: 0
Dernier message: 25/04/2013, 23h19

est-ce les procédures stockées de mysql sont plus rapides que le langage hote ?
Par clavier12AZQSWX dans le forum SQL Procédural
Réponses: 11
Dernier message: 10/09/2012, 04h08

est-ce vrai que les comparaisons de STRING sont plus rapides que les comparaisons de date ou timestamp ?
Par clavier12AZQSWX dans le forum Requêtes
Réponses: 2
Dernier message: 07/03/2012, 17h53

Les pigeons sont plus rapides que l'ADSL en Afrique du Sud, suite à une expérience de l'entreprise locale Unli
Par Katleen Erna dans le forum Actualités
Réponses: 19
Dernier message: 16/09/2009, 08h41

Partager

Nous contacter   Developpez.com   Haut de page