Faille de Sécurité Critique dans Perplexity Comet

Rapport de Veille Technologique

26 novembre 2025

Résumé

Résumé exécutif : Ce document détaille la découverte d'une vulnérabilité majeure dans le navigateur Perplexity Comet, permettant l'injection de prompts indirects via des pages web malveillantes.

Imaginez un pirate informatique capable de contrôler votre navigateur web simplement en cachant des instructions secrètes dans une page internet. C'est exactement ce qu'ont découvert les chercheurs de Brave en août 2025 : une **faille de sécurité majeure dans Perplexity Comet**, le nouveau navigateur boosté à l'intelligence artificielle. Cette vulnérabilité permettait à des personnes malveillantes de manipuler l'IA du navigateur pour voler vos données personnelles, et ce, en toute discrétion.

1 Perplexity Comet : Un Navigateur Piloté par l'IA

Perplexity Comet est un navigateur web nouvelle génération qui utilise l'intelligence artificielle pour vous assister dans vos tâches quotidiennes. Contrairement à Chrome ou Firefox, Comet peut comprendre vos demandes en langage naturel. Par exemple, vous pouvez lui demander "Résume-moi cet article" ou "Trouve-moi les meilleurs restaurants italiens dans ma ville". L'IA analyse alors les pages web et effectue les actions pour vous, de manière autonome.

Cependant, cette autonomie présente un revers de la médaille. En effet, l'IA de Comet lit et interprète tout le contenu des pages web, y compris les parties invisibles pour l'utilisateur. C'est précisément cette caractéristique qu'ont exploitée les chercheurs de Brave pour démontrer la **faille de sécurité de Perplexity Comet**.

2 Comment Fonctionne l'Attaque ?

Le principe de l'attaque est étonnamment simple. Un pirate crée une page web d'apparence normale, mais y cache des instructions malveillantes dans des zones invisibles. Ces instructions peuvent être dissimulées de plusieurs façons :

- **Texte blanc sur fond blanc** : Invisible à l'œil nu, mais lisible par l'IA.
- **Commentaires HTML** : Morceaux de code que les navigateurs classiques ignorent.
- **Balises "spoiler" sur Reddit** : Texte caché jusqu'à ce qu'on clique dessus.
- **Éléments CSS invisibles** : Parties de la page masquées par du code.

Lorsque vous demandez innocemment à Comet de résumer cette page piégée, l'IA lit tout le contenu, y compris les instructions cachées. Le problème majeur : **Comet ne fait pas la différence entre votre demande légitime et les commandes malveillantes du pirate**. L'IA exécute alors les ordres cachés au lieu de simplement résumer la page.

2.1 Un Exemple Concret : L'Attaque Reddit

Les chercheurs de Brave ont démontré un scénario particulièrement inquiétant sur Reddit. Voici comment cela fonctionne :

1. Un pirate publie un message apparemment normal sur un subreddit populaire.
2. Dans ce message, il cache une instruction malveillante dans une balise spoiler.
3. Vous tombez sur ce post et demandez à Comet de vous le résumer.
4. L'IA lit le spoiler caché et exécute la commande du pirate.
5. Résultat : vos données personnelles sont envoyées au pirate sans que vous ne vous en rendiez compte.

3 Quels Sont les Risques pour Vous ?

3.1 Vol de Données Personnelles

La **vulnérabilité de Perplexity Comet** permet potentiellement aux pirates d'accéder à vos conversations avec l'IA. Imaginez toutes les informations confidentielles que vous pourriez avoir partagées : mots de passe, informations bancaires, projets professionnels, ou données personnelles sensibles. Un pirate pourrait demander à Comet d'envoyer tout votre historique vers un serveur sous son contrôle.

3.2 Actions Non Autorisées

Au-delà du vol de données, l'attaque permet de détourner complètement le comportement de Comet. Les chercheurs de Guardio Labs ont même réussi à faire commander une Apple Watch par l'IA sur un faux site e-commerce. L'agent IA peut être manipulé pour :

- Effectuer des achats à votre insu.
- Envoyer des emails en votre nom.
- Visiter des sites de phishing.
- Modifier vos paramètres de sécurité.
- Télécharger des logiciels malveillants.

4 La Réaction de Perplexity

Après que Brave ait signalé la faille de manière responsable en août 2025, Perplexity a publié des correctifs en octobre 2025. L'entreprise a mis en place plusieurs protections incluant le filtrage du contenu web et une meilleure séparation entre vos instructions et le contenu des pages visitées.

Cependant, la situation reste préoccupante. En effet, d'autres chercheurs, notamment chez LayerX, ont découvert des vulnérabilités similaires appelées "CometJacking". De plus, Perplexity a d'abord minimisé l'importance de ces failles, les qualifiant de problèmes "sans incidence sur la sécurité", ce qui a inquiété la communauté des experts en cybersécurité.

5 Un Problème Plus Large : Tous les Navigateurs IA Sont Concernés

Cette faille n'est pas spécifique à Perplexity Comet. En réalité, elle révèle un problème fondamental de tous les navigateurs pilotés par l'IA. Les chercheurs de Guardio Labs ont testé plusieurs navigateurs *agentic* (ChatGPT Atlas, Brave Leo, etc.) et ont constaté que **la plupart sont facilement manipulables**.

Le titre de leur étude est révélateur : *"Nous avons testé les navigateurs IA - Ils ont cliqué, ils ont payé, ils ont échoué"*. Selon eux, les cybercriminels n'auront bientôt plus besoin de tromper les utilisateurs : **il leur suffira de tromper les IA**.

6 Comment Se Protéger ?

Si vous utilisez Perplexity Comet ou un navigateur similaire, voici quelques précautions essentielles :

- **Méfiez-vous des sites inconnus** : Ne demandez pas à l'IA de résumer des pages provenant de sources douteuses.
- **Limitez les permissions** : N'autorisez pas Comet à accéder à vos comptes sensibles (email, banque).
- **Vérifiez les actions** : Avant de valider une action suggérée par l'IA, vérifiez toujours qu'elle correspond à votre demande.
- **Surveillez vos comptes** : Gardez un œil sur toute activité suspecte.
- **Attendez la maturité du produit** : Ces outils sont encore en développement et présentent des risques importants.

7 L'Avis des Experts

Les spécialistes en cybersécurité sont unanimes : les navigateurs IA arrivent trop tôt sur le marché. Comme l'explique Guardio Labs, *"à l'ère de l'IA contre l'IA, les escrocs n'ont pas besoin de tromper des millions de personnes différentes ; ils n'ont besoin que de casser un modèle d'IA"*.

Par ailleurs, les préoccupations concernant la vie privée s'ajoutent aux problèmes de sécurité. Le PDG de Perplexity, Aravind Srinivas, a ouvertement admis que l'objectif de Comet est de **collecter un maximum de données sur vos activités en ligne pour vendre de la publicité ciblée**. Combiné aux failles de sécurité, cela crée un cocktail particulièrement risqué pour votre vie privée.

8 Que Retenir de Cette Affaire ?

La **faille de sécurité découverte dans Perplexity Comet** par Brave illustre les dangers des technologies d'IA déployées trop rapidement. Alors que ces outils promettent de révolutionner

notre façon de naviguer sur internet, ils introduisent de nouveaux risques que nous commençons à peine à comprendre.

Cette histoire nous rappelle qu'il faut toujours rester vigilant face aux nouvelles technologies, surtout lorsqu'elles nous demandent des accès étendus à nos données personnelles. Par conséquent, avant d'adopter un navigateur piloté par l'IA, posez-vous la question : les avantages valent-ils vraiment les risques ?

Et vous, utiliseriez-vous un navigateur contrôlé par une intelligence artificielle ?