AYI NEDJIMI
Consultants

Faille Microsoft 365 Copilot Permet l'Exfiltration de

15 octobre 2025 • Mis à jour le 17 mai 2026 • 5 min de lecture •

1532 mots • 749 vues •

Exfiltration de. Expert en cybersécurit'exfiltrer des données sensibles en exploitant les capacités d'IA de l'assistant.

La veille cybersécurité permanente est devenue une nécessité opérationnelle pour les équipes de sécurité, permettant d'anticiper les nouvelles menaces, de prioriser les actions de remédiation et d'adapter les stratégies de défense en temps réel. L'actualité de la cybersécurité est marquée par une accélération sans précédent des menaces, des vulnérabilités et des incidents affectant organisations et particuliers à l'échelle mondiale. Les équipes de sécurité doivent maintenir une veille permanente pour anticiper les risques émergents, appliquer les correctifs critiques et adapter leurs stratégies de défense. Cette analyse décrypte les derniers événements marquants du paysage cyber et leurs implications concrètes pour la protection de vos systèmes d'information. À travers l'analyse de **Faille Microsoft 365 Copilot Permet l'Exfiltration**, nous vous proposons un décryptage complet des enjeux et des solutions à mettre en œuvre.

📋 **EN BREF**

- ▶ Contexte et chronologie des événements
- ▶ Impact sur l'écosystème cybersécurité
- ▶ Leçons apprises et recommandations
- ▶ Perspectives et évolutions attendues

Microsoft 365 **Vulnérabilité** **IA** 23 octobre 2025 à 08:45

Par **Ayi NEDJIMI**

Faille Critique dans Microsoft 365 Copilot Permet l'Exfiltration de Données Sensibles

> Des chercheurs en sécurité ont découvert une vulnérabilité majeure dans Microsoft 365 Copilot permettant aux attaquants d'exfiltrer des données confidentielles d'entreprise en exploitant les capacités d'IA de l'assistant. Cette faille expose les organisations utilisant Copilot à des risques de fuite de données critiques.