

CVE-2025-64446 : Faille Critique FortiWeb CVSS 9.8

📅 6 octobre 2025 • 🔄 Mis à jour le 17 mai 2026 • ⌚ 4 min de lecture •
☰ 1189 mots • 👁 1024 vues • ❤

Analyse de la vulnérabilité critique CVE-2025-64446 affectant FortiWeb avec un score CVSS de 9.8, permettant une execution de code a distance sans authentification.

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 et appliquer les correctifs critiques et adapter leurs stratégies.

Reportage 24/7

Devis
gratuit



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 **CVE-2025-64446 : Faille Critique FortiWeb CVSS 9.8**, 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

CVE-2025-64446 : Faille Critique FortiWeb CVSS 9.8 — Analyse de la vulnérabilité critique CVE-2025-64446 affectant FortiWeb avec un score CVSS de 9.8, permettant une exécution de code à distance sans authentification. Cette actualité s'inscrit dans un contexte de menaces croissantes où la vigilance des équipes de sécurité est plus que jamais nécessaire.

À RETENIR

Un projet cybersécurité ?
Réponse sous 24h

Devis
gratuit →

Réponse sous 24h

Devis
gratuit →