



BadSuccessor : Nouvelle Faille Critique Windows AD

11 décembre 2025 • Mis à jour le 17 mai 2026 • 4 min de lecture • 1167 mots • 786 vues •

La vulnérabilité BadSuccessor permet une escalade de privileges dans Active Directory via les comptes DMSA. Microsoft publie un correctif.



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.

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 **BadSuccessor : Nouvelle Faille Critique Windows AD**, 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

BadSuccessor : Nouvelle Faille Critique Windows AD — La vulnérabilité BadSuccessor permet une escalade de privilèges dans Active Directory via les comptes DMSA. Microsoft publie un correctif. Cette actualité s'inscrit dans un contexte de menaces croissantes où la vigilance des équipes de sécurité est plus que jamais nécessaire.

À RETENIR

Les Faits

L'événement a été confirmé par plusieurs sources

indépendantes. Les équipes de sécurité du monde

surveillent la situation de près. Les indicateurs

Un projet cybersécurité ?
Réponse sous 24h

Devis
gratuit →

Réponse sous 24h

Devis
gratuit →