Faille critique dans Microsoft Entra ID

Microsoft Entra ID, anciennement Azure Active Directory, est la solution de Microsoft pour gérer les identités et les accès dans le cloud. En juin 2025, un chercheur a découvert une faille critique permettant à des attaquants d'usurper l'identité de n'importe quel utilisateur, y compris celle d'un administrateur global, et de prendre le contrôle complet de l'environnement cloud d'une organisation. Bien que corrigée rapidement, cette vulnérabilité illustre les risques liés aux mécanismes hérités encore présents dans certaines infrastructures. En quoi cette faille révèle-t-elle les dangers liés à la gestion des identités dans le cloud ?

Le problème venait d'une combinaison entre des jetons internes appelés *Actor Tokens*, utilisés par Microsoft pour permettre à certains services de se faire passer pour un utilisateur. Un attaquant pouvait alors créer un jeton dans son propre tenant et l'utiliser dans un autre pour se faire passer pour un administrateur global. Il lui suffisait de connaître l'identifiant du tenant, public, et le netId d'un utilisateur, récupérable par force brute ou via un compte invité. Avec cela, il pouvait contrôler entièrement l'environnement : accéder aux données, créer de nouveaux comptes, installer des portes dérobées, étendre son accès à Microsoft 365, et tout cela sans être bloqué par l'authentification multi facteur ni laisser de traces dans les journaux. Alerté en juillet 2025, Microsoft a déployé un correctif en moins d'une semaine. Celui-ci a bloqué l'usage des Actor Tokens avec Azure AD Graph et introduit des mesures de sécurité supplémentaires. L'éditeur a également insisté sur la nécessité d'abandonner les anciennes API au profit de Microsoft Graph, plus sécurisé.

Cette faille démontre que la gestion des identités est un point central de la cybersécurité et une surface d'attaque à part entière. Même corrigée, elle rappelle que les entreprises doivent limiter l'usage de solutions héritées, renforcer la surveillance de leurs environnements cloud et traiter la sécurité des identités avec autant d'importance que la protection des données et des applications.

Sources

https://www.lemondeinformatique.fr/actualites/lire-microsoft-et-cloudflare-frappent-le-cybergang-raccoono365-97906.html

https://www.it-connect.fr/entra-id-actor-tokens-vulnerabilite-cve-2025-55241/