Sécurité : Microsoft Active Directory victime d'une faille critique

L'entreprise israélienne de sécurité **Aorato** annonce avoir découvert une faille critique dans **Microsoft Active Directory**. Celle-ci permet à l'attaquant de **changer le mot de passe de l'utilisateur**. *« Alors que 95% des entreprises du Fortune 1000 ont déployé Active Directory, nous considérons cette vulnérabilité comme hautement sensible »*, indique la firme spécialisée sur le service d'annuaire de Redmond dans un billet de blog qui détaille la méthodologie de l'attaque.

Active Directory s'appuie de fait sur **NTLM**, un « vieux » protocole d'identification utilisé par défaut jusqu'à Windows XP SP3 mais dont Microsoft conserve la compatibilité avec ses OS plus récents malgré l'implémentation de Kerberos depuis Windows 2000. Or, NTLM est victime d'une vulnérabilité connue, baptisée «**pass-the-hash**» (PtH, contourner la vérification par hachage d'une donnée), qui permet à un attaquant d'obtenir des informations de connexion. Et Aorato, soutient qu'il suffit d'utiliser des outils de tests d'intrusion comme WCE ou Mimikatz pour obtenir le hash du protocole NTLM et déterminer les identifiants de connexion afin de changer le mot de passe d'un utilisateur.

Porte ouverte à d'autres services

Au-delà des informations et données de la victime que les attaquants peuvent recueillir, la vulnérabilité ouvre l'accès à d'autres services du réseau de l'entreprise comme le **Remote Desktop Protocol** (RDP), le protocole de gestion à distance des postes Windows, et **Outlook Web Access** (OWA), l'application de messagerie professionnelle multiplateforme et mobile. De plus, l'usurpation d'identité rendra transparente l'attaque aux yeux des systèmes de sécurité.

Aorato a alerté Microsoft de l'existence de cette vulnérabilité. Si l'éditeur a reconnu le risque d'intrusion, il le considère comme **une *« limite »* qu'il ne peut corriger** car directement liée à la conception du protocole d'identification NTLM dont les spécifications sont publiquement accessibles. De fait, Microsoft estime que la faiblesse du protocole l'est aussi et que les entreprises en sont donc conscientes. De plus, la firme de Redmond a publié une mise à jour en mai 2014 pour ses versions de Windows desktop 7 et 8.x, et serveur (Server 2008 R2 et plus) renforçant la protection des informations d'identité et de contrôle d'identification. Enfin, Microsoft préconise l'usage d'authentification par carte à puce et la suppression de RC4-HMAC (méthode de chiffrement de Kerberos qui assure la rétrocompatibilité) des systèmes. Deux solutions que Aorato ne voit pas comme *« viables et pratiques »*.

Une erreur d'implémentation

Dans tous les cas, la firme israélienne considère la faille du hash NTLM comme une erreur d'implémentation (« by-design » flaw) dans Active Directory. De plus, *« alors que Microsoft considère cette limite de conception du protocole comme publique et « bien connue », c'est* ***la combinaison des différents aspects qui fait de cette révélation une nouveauté*** *»*, ajoute Aorato qui fait référence à la

fois à la faille de NTLM, à l'usage des outils de tests d'intrusion pour déterminer les identifiant de connexion et la capacité à passer inaperçu pour l'attaquant qui les exploite.

« Puisqu'il n'y a pas de solution inhérente, ***la protection doit être fournie depuis l'extérieur*** *»*, souligne Aorato qui préconise un ensemble de mesures comme détection de l'usage d'un algorithme de chiffrement alternatif à celui implémenté par défaut, l'identification de l'attaque par corrélation entre l'utilisation « anormale » de la méthode de chiffrement et son contexte (date et heure inhabituelles au regard du profil utilisateur habituel, etc.), réduire la surface de l'attaque, etc. A noter néanmoins que Microsoft propose également sa méthode pour limiter l'attaque «Pass-the-hash».

crédit photo © Pavel Ignatov – shutterstock

Lire également

Un algorithme de compression corrige une faille vieille de 20 ans
Une faille du WiFi d'Android dévoile les données personnelles
Le greffon Flash d'Adobe au cœur d'une attaque d'envergure