Les chercheurs de Preempt découvrent deux vulnérabilités critiques dans Microsoft NTLM, permettant l'exécution à distance de codes malveillants sur toute machine Windows

Trois failles du protocole d'authentification propriétaire de Microsoft permettent aux pirates de contourner tous les mécanismes de protection NTLM

SAN FRANCISCO, 12 juin 2019 (GLOBE NEWSWIRE) — Preempt, le principal fournisseur d'accès conditionnel pour la prévention des menaces en temps réel, a annoncé aujourd'hui que son équipe de recherche avait découvert deux vulnérabilités critiques pour Microsoft, consistant en trois failles logiques dans NTLM, le protocole d'authentification propriétaire de la société. Ces vulnérabilités permettent aux pirates d'exécuter à distance un code malveillant sur n'importe quel ordinateur Windows ou de s'authentifier sur tout serveur Web prenant en charge l'authentification Windows intégrée (WIA), tel qu'Exchange ou ADFS. La recherche montre que toutes les versions de Windows sont vulnérables.

NTLM est susceptible de relayer les attaques, ce qui permet aux acteurs de capturer une authentification et de la relayer vers un autre serveur, et ainsi d'effectuer des opérations sur le serveur distant en utilisant les privilèges de l'utilisateur authentifié. Le relais NTLM est l'une des techniques d'attaque les plus courantes utilisées dans les environnements Active Directory, dans lesquels le pirate parvient à compromettre un ordinateur, puis se déplace latéralement vers d'autres ordinateurs à l'aide de l'authentification NTLM sur le serveur compromis.

Microsoft avait précédemment mis au point plusieurs mesures d'atténuation pour empêcher les attaques par relais NTLM. Les chercheurs de Preempt ont découvert que ces mesures d'atténuation présentaient les failles suivantes qui pourraient être exploitées par des pirates :

- Le champ MIC (Message Integrity Code) garantit que les pirates n'altèrent pas les messages NTLM. Le contournement découvert par les chercheurs de Preempt permet aux pirates de supprimer la protection « MIC » et de modifier divers champs du flux d'authentification NTLM, tels que la négociation de signature.
- La signature de session SMB empêche les pirates de relayer les messages d'authentification NTLM pour ouvrir des sessions SMB et DCE/RPC. Le contournement découvert par les chercheurs de Preempt permet aux pirates de relayer les demandes d'authentification NTLM vers n'importe quel serveur du domaine, y compris les contrôleurs de domaine, tout en établissant une session signée pour l'exécution de code à distance. Si l'authentification relayée est celle d'un utilisateur privilégié, cela signifie une compromission totale du domaine.
- La protection améliorée pour l'authentification (EPA) empêche les pirates de relayer les

messages NTLM aux sessions TLS. Le contournement découvert par les chercheurs de Preempt permet aux pirates de modifier les messages NTLM afin de générer des informations de liaison de canal légitimes. Cela permet aux pirates de se connecter à divers serveurs Web en utilisant les privilèges de l'utilisateur attaqué et d'effectuer des opérations telles que lire les courriels de l'utilisateur (en les relayant vers des serveurs OWA) ou même se connecter à des ressources sur le cloud (en relayant vers des serveurs ADFS).

Pour plus de détails sur les risques signalés de ces failles, veuillez visiter le blog d'avis de sécurité de Preempt ici.

« Même si le relais NTLM est une technique ancienne, les entreprises ne peuvent pas éliminer complètement l'utilisation du protocole, car de nombreuses applications en souffriraient. Il présente donc toujours un risque important pour les entreprises, en particulier avec la découverte constante de nouvelles vulnérabilités », a déclaré Roman Blachman, directeur technique et co-fondateur de Preempt. « Les entreprises doivent avant tout garantir que tous leurs systèmes Windows soient corrigés et sécurisés. En outre, les organisations peuvent renforcer la protection de leurs environnements en obtenant une visibilité réseau NTLM. Preempt collabore avec ses clients pour leur assurer cette visibilité et la meilleure protection possible. »

Pour se protéger de ces vulnérabilités, les organisations doivent :

1. Correctif : s'assurer que les postes de travail et les serveurs sont correctement corrigés. Cependant, il est important de noter que les correctifs ne suffisent pas ; il est également nécessaire que les entreprises apportent des modifications à la configuration pour être totalement protégées.
2. Configuration :
    A. Appliquer la signature SMB : pour empêcher les pirates de lancer des attaques plus simples par relais NTLM, activer la signature SMB sur toutes les machines du réseau.
    B. Bloquer NTLMv1 : NTLMv1 étant considéré comme nettement moins sécurisé, il est recommandé de le bloquer complètement en définissant le GPO approprié.
    C. Appliquer la signature LDAP/S : afin d'empêcher le relais NTLM dans LDAP, appliquer la signature LDAP et la liaison de canal LDAPS sur les contrôleurs de domaine.
    D. Appliquer l'EPA : pour empêcher le relais NTLM sur les serveurs Web, renforcer tous les serveurs Web (OWA, ADFS) pour qu'ils acceptent uniquement les demandes avec EPA.
3. Réduire l'utilisation de NTLM : même avec une configuration entièrement sécurisée et des serveurs corrigés, NTLM présente un risque considérablement plus important que Kerberos. Il est recommandé de supprimer NTLM là où il n'est pas nécessaire.

Les clients de Preempt disposent déjà de protections contre les vulnérabilités NTLM. La plate-forme Preempt offre une visibilité NTLM réseau complète, permettant aux organisations de réduire le trafic NTLM et d'analyser les activités NTLM suspectes. En outre, Preempt dispose d'une capacité innovante de détection de relais NTLM déterministe, une première dans le secteur, et est en mesure d'inspecter toutes les configurations de GPO. Il alerte également en cas de configuration

non sécurisée. Cette inspection de la configuration est également disponible dans Preempt Lite, une version légère et gratuite de la plate-forme Preempt. Les organisations peuvent télécharger Preempt Lite ici et vérifier quelles zones de leur réseau sont vulnérables.

Ces vulnérabilités et d'autres seront présentées par les chercheurs de Preempt Yaron Zinar et Marina Simakov lors de la conférence Black Hat USA 2019.

Au 11 juin 2019, Microsoft a publié les correctifs CVE-2019-1040 et CVE-2019-1019 le mardi après la divulgation responsable par Preempt des vulnérabilités de NTLM.

À propos de Preempt
Preempt offre une approche moderne de l'authentification et de la sécurisation de l'identité dans l'entreprise. Grâce à la technologie brevetée d'accès conditionnel, Preempt aide les entreprises à optimiser la bonne santé des identités et à mettre fin aux attaques en temps réel avant qu'elles n'affectent les activités. Preempt détecte et prévient en permanence les menaces en fonction de l'identité, du comportement et des risques sur toutes les plates-formes d'authentification et d'accès au cloud et sur site. Cette approche à faible coefficient de friction donne aux équipes de sécurité plus de visibilité et de contrôle sur les comptes et les accès privilégiés, tout en garantissant la conformité et la résolution automatique des incidents. Pour en savoir plus, visitez le site www.preempt.com.

ou contactez
Angelique Faul
Angelique@silverjacket.net
513-633-0897