

CAS D'UTILISATION 10

Remote Desktop Manager + Devolutions Server + Gestion d'accès privilégiés

Remplacer Remote Credential Guard par le PAM de Devolutions

Comment faire en sorte que vos identifiants soient moins exposés aux serveurs RDP de destination en utilisant le PAM de Devolutions plutôt que Remote Credential Guard.

Le public cible

Ce cas d'utilisation s'adresse aux organisations soucieuses de la sécurité et qui s'efforcent d'atténuer l'action des mauvais acteurs qui cherchent à voler les identifiants du protocole de Bureau à distance (RDP) à des fins d'élévation des privilèges ou d'attaques latérales de l'infrastructure.

L'enjeu

Microsoft Remote Credential Guard (RCG), la solution traditionnelle de protection des informations d'identification RDP « en mémoire », présente des limites qui ne conviennent pas à toutes les organisations. En plus, RCG limite les types d'informations d'identification disponibles et certaines tâches informatiques communes, comme la délégation d'accès ou l'utilisation de comptes de services dans l'automatisation.

La solution

Comment une organisation peut-elle protéger les informations d'identification RDP en mémoire tout en conservant une certaine flexibilité? Une solution unique de gestion des accès privilégiés (PAM) réinitialise de manière transparente les mots de passe à chaque sortie d'une session RDP, ce qui mitige l'exploitation future des identifiants RDP. En outre, il n'est pas nécessaire de transmettre les informations de connexion aux employés, puisque chaque authentification est unique. Il n'est pas non plus nécessaire de réinitialiser les mots de passe au moment de la sortie.

Le fonctionnement

Étape 1: [Activez la gestion des accès privilégiés](#) à partir de l'interface Web de Devolutions Server.

Étape 2: Configurez les fournisseurs et importez les comptes à gérer.

Étape 3: Ajoutez des entrées aux coffres liés aux comptes d'accès privilégiés.

Étape 4: Une fois que l'utilisateur final termine la session, les mots de passe sont automatiquement réinitialisés, ce qui réduit les risques d'attaque.

Résumé des avantages

- **Surface d'attaque réduite** : comme les mots de passe sont changés chaque fois, toute exploitation ultérieure devient impossible.
- **Flexibilité accrue** : contrairement à RCG, le module de gestion d'accès privilégiés conserve les mêmes processus et capacités qu'auparavant, mais avec la sécurité accrue de la rotation automatique des mots de passe.
- **Maintenance réduite** : sans la nécessité d'alterner les mots de passe des employés à chaque sortie de session, on gagne du temps et on n'interrompt pas les processus existants.

Prochaines étapes

Découvrez comment Devolutions peut aider votre organisation à renforcer la sécurité, à assurer la conformité et à améliorer la gestion des utilisateurs :

- **Demandez un essai gratuit de Devolutions Server** – [cliquez ici](#)
- **Demandez un essai gratuit de Remote Desktop Manager** – [cliquez ici](#)
- **Demandez une démonstration en direct de Remote Desktop Manager** – [cliquez ici](#)
- **Communiquez avec nous pour plus d'informations** – [cliquez ici](#)