GENDARMERIE NATIONALE
PÔLE NATIONAL DE LUTTE CONTRE LES CYBERMENACES

CYBERGEND

BRIGADE numérique
Pour toute question, 24h/24, 7j/7 :
www.contacterlagendarmerie.fr/
En cas d'urgence, contactez le 17

Note d'information #CyberGend
Date: 2020/04/22
Numéro: 2020-113A

OBJET: COVID-19 – Vulnérabilités des systèmes de partage de bureau à distance

Exploitation d'accès RDP faiblement protégés

Dans le cadre de la crise pandémique du **COVID-19** un grand nombre d'organisations ont mis en place des solutions de **travail à distance** reposant sur des fonctionnalités de partage de bureau, parfois dans la précipitation, entrainant des risques supplémentaires d'accès par des acteurs malveillants.

La gendarmerie nationale a constaté qu'un grand nombre de structures de tailles variées (entreprises, collectivités locales, professions libérales) utilisent actuellement des solutions de type Microsoft Windows ***Remote Desktop Protocol*** **(RDP)** susceptibles d'être exploitées par des cybercriminels.

Lorsque le contrôle d'accès est trop faible (identifiant générique, **mot de passe faible**, absence d'utilisation d'un certificat de sécurité), les attaquants peuvent facilement identifier un tel accès, s'introduire dans la machine et le réseau local, extraire des **données confidentielles** et installer un **rançongiciel**. Ces vulnérabilités sont activement exploitées depuis le début du confinement.

L'utilisation d'un port différent du port par défaut (3389) n'empêche pas les attaquants de découvrir l'existence de votre serveur.

Recommandations
pour le service informatique ou le prestataire

- Assurez-vous de **respecter les recommandations de l'ANSSI**[1] **en matière de solidité et de renouvellement des mots de passe** et celles touchant à la sécurité des services de bureau à distance[2].
- Si vous n'utilisez pas votre serveur RDP, désactivez-le et vérifiez les règles de votre pare-feu
- Assurez-vous de n'autoriser des accès distants que pour des utilisateurs ne disposant pas de droits d'administration.
- Fermez les accès distants des utilisateurs qui n'ont pas ou plus besoin de l'utiliser.
- Activez le protocole d'authentification par le réseau *Network Level Authentication* (NLA) – dans ce cas attention à ne pas activer la fonction qui force le renouvellement du mot de passe à la prochaine connexion
- Mettez en place des règles de filtrage géographique ou par adresse IP
- Mettez en place des règles permettant d'identifier une utilisation suspecte (essais répétés, adresse IP inhabituelle, etc.)

1. https://www.ssi.gouv.fr/guide/mot-de-passe/
2. https://www.cert.ssi.gouv.fr/alerte/CERTFR-2019-ALE-006/

Pour obtenir de l'assistance en cas d'atteinte à votre système d'information, contactez notre partenaire

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique