Vulnérabilité critique affectant le service « Remote Desktop Protocol » (RDP) de Windows

Les Technologies de l'information souhaitent informer les responsables informatiques que Microsoft a diffusé, lors de la publication des correctifs mensuels du mois de mai 2019, un avis de sécurité concernant une **vulnérabilité critique** affectant le service « *Remote Desktop Protocol (RDP)* ».

Cette vulnérabilité critique affecte le service de bureau à distance (anciennement connu sous le nom « services de terminal »). Elle peut être exploitée à distance, par le réseau, à l'aide de requêtes malveillantes sur un système vulnérable utilisant le protocole « RDP ». De plus, l'exploitation de cette faille ne nécessite aucune authentification.

Cette vulnérabilité affecte les versions du système d'exploitation *Windows 7*, *Windows Server 2008 R2*, *Windows Server 2008* ainsi que les versions *Windows 2003* et *Windows XP* qui ne possèdent plus de support officiel pour les correctifs de sécurité.

Veuillez noter que les versions du système d'exploitation *Windows 8*, *Windows 10*, *Windows Server 2012*, *Windows 2012 R2*, *Windows Server 2016* et *Windows Server 2019* **ne sont pas affectées** par cette vulnérabilité.

Microsoft a publié des correctifs pour les systèmes d'exploitation vulnérables. Pour le téléchargement, veuillez consulter les liens ci-dessous :

- *Correctifs de support pour Windows 7 et Windows 2008 :*
  - https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708
- *Correctifs hors cycle de vie/support pour Windows (Windows XP, Windows 2003) :*
  - https://support.microsoft.com/en-us/help/4500705/customer-guidance-for-cve-2019-0708

Veuillez prendre connaissance des mesures d'atténuation recommandées :

- Installer les mises à jour les plus récentes des systèmes d'exploitation vulnérables.
- Désactiver les services « Bureau à distance » lorsqu'il n'est plus utilisé. Au besoin, surveiller les activités suspectes dans le trafic réseau et les journaux des systèmes vulnérables.
- Activer l'authentification au niveau du réseau (NLA) sur les systèmes qui exécutent *Windows 7*, *Windows Server 2008* et *Windows Server 2008 R2*. Il s'agit d'une atténuation partielle qui empêchera la propagation du logiciel malveillant. De plus, lorsque l'authentification NLA est activée, un attaquant devra s'authentifier à l'aide d'un compte valide sur le système cible.
- Bloquer le port TCP 3389 sur le coupe-feu (« firewall ») lorsque possible. Cette mesure empêchera tout accès non autorisé provenant d'Internet.

Pour plus d'information concernant cette vulnérabilité critique, veuillez consulter les liens suivants :

- https://cyber.gc.ca/fr/avis/vulnerabilite-critique-du-bureau-distance-de-microsoft
- CVE-2019-0708 : https://blogs.technet.microsoft.com/msrc/2019/05/14/prevent-a-worm-by-updating-remote-desktop-services-cve-2019-0708/

Pour toutes questions d'ordre technique, veuillez communiquer avec l'équipe *Sécurité* des Technologies de l'information, par courriel à l'adresse « securite @umontreal.ca ».

Les Technologies de l'information vous remercient de votre collaboration.

(16 mai 2019)