Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ÉCONOMIE
ET DES FINANCES

MINISTÈRE DE L'ACTION
ET DES COMPTES PUBLICS

SECRÉTARIAT GÉNÉRAL

Paris, le 31 MAI 2019

SERVICE DU HAUT FONCTIONNAIRE DE DEFENSE ET DE SECURITE
TELEDOC 722
120 RUE DE BERCY
75572 PARIS CEDEX 12

N°SHFDS/2019/05/10160

NOTE POUR
MESDAMES ET MESSIEURS LES DIRECTEURS, OFFICIERS,
DELEGUES ET RESPONSABLES DE SECURITE

Objet : Adaptation en urgence du domaine de la sécurité du numérique de la posture Vigipirate « Eté – Rentrée 2019 ».

Annexe : Adaptation du domaine de la sécurité du numérique.

La posture VIGIPIRATE « *Eté – Rentrée 2019* » est active depuis le 7 mai 2019. Elle continue de s'appliquer, sauf événement particulier, jusqu'au 18 octobre 2019, veille des vacances de la Toussaint.

Le 14 mai 2019, lors de sa mise à jour mensuelle, MICROSOFT a publié un correctif de sécurité pour une vulnérabilité sur un service de prise en main à distance Windows appelé *Remote Desktop Services* (RDS).

Au regard du risque particulièrement important qui découlerait de l'exploitation de cette vulnérabilité, une adaptation en urgence du domaine de la sécurité du numérique de la posture VIGIPIRATE « *Eté – Rentrée 2019* » se révèle nécessaire.

Il vous est demandé de diffuser cette adaptation du domaine de la sécurité du numérique de la posture Vigipirate « *Eté – Rentrée 2019* » à l'ensemble de vos services ou adhérents, **sans que cela ne se traduise par une publication en accès libre sur vos sites internet.**

Pour le Haut fonctionnaire de défense et de sécurité adjoint

Philippe ARMAND

Annexe 1 : Adaptation du domaine de la sécurité du numérique

1. Contexte général

Le 14 mai 2019, lors de sa mise à jour mensuelle, Microsoft a publié un correctif de sécurité pour une vulnérabilité sur un service de prise en main à distance Windows appelé Remote Desktop Services (RDS). Cette vulnérabilité est jugée critique dans la mesure où elle permet d'exécuter à distance des codes malveillants, sans authentification ni interaction avec un utilisateur.

Cette vulnérabilité touche les systèmes d'exploitation Windows, postes de travail et serveurs, jusqu'à Windows 7 et Windows Server 2008 R2. Ces versions, dont le support est assuré par l'éditeur jusqu'au 14 janvier 2020, sont très largement déployées.

De par le risque particulièrement important qui découlerait de l'exploitation de cette vulnérabilité, MICROSOFT a également rendu disponibles des mises à jour exceptionnelles pour les anciens systèmes n'étant normalement plus pris en charge.

Dans la mesure où l'exploitation de cette faille pourrait permettre la création d'un ver informatique – de type Wannacry ou NotPetya – particulièrement virulent, **il est décidé d'adapter le domaine de la sécurité du numérique de la posture Vigipirate selon les modalités précisées ci-dessous.**

À la date du 24 mai 2019, aucun code d'exploitation permettant une exploitation automatisée de cette faille n'est disponible publiquement. Néanmoins, plusieurs sources fiables affirment l'existence de tels codes, rendant crédible la matérialisation de ce risque. Les équipes de l'ANSSI ont par ailleurs réussi à développer une preuve de concept en quelques heures.

2. Activation et modification de mesures de sécurité du numérique de la posture Vigipirate en vigueur

Dans ce contexte, l'adaptation du domaine de la sécurité numérique de la posture Vigipirate se matérialise par les deux mesures suivantes, qui s'appliquent sur l'ensemble des systèmes d'exploitation Windows XP, Windows Server 2003, Windows Vista, Windows 7, Windows Server 2008 et Windows Serveur 2008 R2 présents sur le parc informatique.

- « Valider et appliquer un correctif de sécurité » :

  Les correctifs de sécurité correspondant aux bulletins du CERT-FR mentionnés ci-dessous doivent impérativement être appliqués pour corriger des vulnérabilités récentes particulièrement critiques :

  - CERTFR-2019-ALE-002 (www.cert.ssi.gouv.fr/alerte/CERTFR-2019-ALE-002) – Vulnérabilités affectant l'écosystème MICROSOFT Exchange et Active Directory

  - CERTFR-2018-ALE-013 (www.cert.ssi.gouv.fr/alerte/CERTFR-2018-ALE-013) – Vulnérabilité dans MICROSOFT Internet Explorer

  - CERTFR-2019-AVI-090 (www.cert.ssi.gouv.fr/avis/CERTFR-2019-AVI-090) – Multiples vulnérabilités dans GOOGLE Chrome

- CERTFR-2019-ALE-006 (www.cert.ssi.gouv.fr/avis/CERTFR-2019-ALE-006) – Vulnérabilité dans MICROSOFT Remote Desktop Services (se référer à ce bulletin pour obtenir les informations techniques nécessaires à la mise en œuvre de cette mesure)

– « Définir un paramètre de configuration sur un logiciel/service/système d'exploitation » :

Il s'agit d'activer l'authentification Network Level Authentication (NLA) sur l'ensemble du parc[1]. Cette fonctionnalité permet d'éviter l'exploitation en préauthentification en forçant une authentification du client lors de l'initialisation de la connexion RDP.

[1] Au vu de la capacité d'exploitation préauthentification de la vulnérabilité, il est nécessaire de réaliser un travail d'identification complémentaire des postes non attachés à un domaine, qui seraient potentiellement vulnérables.