Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ÉCONOMIE
ET DES FINANCES

MINISTÈRE DE L'ACTION
ET DES COMPTES PUBLICS

SECRÉTARIAT GÉNÉRAL

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

Paris, le 24 JAN. 2020

N°SHDS/2020/01/7531

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

Objet : Adaptation en régularisation du domaine de la sécurité du numérique de la posture Vigipirate « *Automne hiver 2019 – Printemps 2020* ».

Annexe : Adaptation du domaine de la sécurité du numérique.

La posture Vigipirate « Automne hiver 2019 – Printemps 2020 » est active depuis le 18 octobre 2019. Elle s'applique, sauf évènement particulier, jusqu'au 14 mai 2020.

Les 9 et 13 janvier 2020, le CERT-FR a alerté sur des campagnes de détection **et la publication de codes permettant l'exploitation d'une vulnérabilité** affectant des logiciels Citrix.

Le 14 janvier 2020, lors de sa mise à jour mensuelle, Microsoft a publié deux correctifs de sécurité pour de multiples vulnérabilités critiques identifiées sur Windows. Ces vulnérabilités affectent de multiples versions du système d'exploitation, dont plusieurs versions destinées aux serveurs, **augmentant ainsi fortement la surface d'attaque des systèmes concernés**. En outre, une des vulnérabilités affecte les mécanismes de contrôle de la confiance dans le système de mise à jour de Microsoft et dans certains protocoles de communication sécurisés très répandus, la rendant particulièrement critique.

Si les démarches ont été entreprises par la chaine « sécurité des systèmes d'information », **une régularisation du domaine de la sécurité du numérique de la posture Vigipirate « Automne hiver 2019 – printemps 2020 » se révèle nécessaire** pour mieux sensibiliser tous les acteurs au risque particulièrement important qui découlerait de l'exploitation de ces vulnérabilités.

Une description du contexte général et la mise à jour apportée aux mesures de sécurité du numérique de la posture VIGIPIRATE en vigueur sont présentées en annexe.

Il vous est demandé de diffuser cette adaptation du domaine de la sécurité du numérique de la posture Vigipirate « Automne hiver 2019 – Printemps 2020 » à l'ensemble de vos services ou adhérents, sans que cela ne se traduise par une publication en accès libre sur vos sites internet.

Le Haut fonctionnaire de défense et de sécurité adjoint

Christian DUFOUR

Annexe : Adaptation du domaine de la sécurité du numérique

1. Contexte général

Le 14 janvier 2020, MICROSOFT a publié des correctifs de sécurité pour deux vulnérabilités affectant plusieurs versions du système d'exploitation Windows, dont des versions destinées aux serveurs :

- CVE-2020-0601, vulnérabilité affectant **un composant cryptographique** permettant de sécuriser des applications Windows en implémentant des fonctions relatives aux certificats de sécurité et messageries chiffrées. L'exploitation de cette vulnérabilité pourrait notamment permettre à des attaquants de contourner discrètement les mesures de sécurité en place en faisant passer pour légitime un programme malveillant signé à l'aide d'un certificat falsifié, d'usurper l'identité d'un utilisateur ou d'un serveur lors de l'établissement d'une connexion sécurisée (TLS) ou d'usurper l'identité de l'émetteur d'un message électronique signé.

- CVE-2020-0610 et CVE-2020-0609, vulnérabilités permettant l'accès à distance à un serveur. L'exploitation de ces vulnérabilités pourrait permettre à un attaquant de se connecter sans authentification à un système utilisant une version vulnérable du protocole et d'y exécuter un programme malveillant à distance.

Par ailleurs, le CERT-FR a récemment alerté sur **des campagnes de détection de la vulnérabilité CVE-2019-19781 affectant des logiciels Citrix** permettant d'accéder à distance aux systèmes d'information qui en sont équipés. Ces campagnes de détection correspondent à des phases de reconnaissance préalables à une intrusion. L'exploitation de cette vulnérabilité pourrait en effet permettre l'exécution à distance d'un programme malveillant sur le système ciblé. Des codes permettant une telle exploitation ont été publiés sur Internet dans la nuit du 10 au 11 janvier 2020 et leur mise en œuvre aurait déjà été rapportée par la presse.

Dans la mesure où l'exploitation de ces vulnérabilités pourrait permettre des atteintes graves aux systèmes d'information visés, **il est décidé d'adapter le domaine de la sécurité du numérique de la posture VIGIPIRATE selon les modalités précisées ci-dessous.**

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

– *« Valider et appliquer un correctif de sécurité »* est **adaptée**.

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

- **CERTFR-2020-ALE-004** (www.cert.ssi.gouv.fr/alerte/CERTFR-2020-ALE-004) – **Vulnérabilité dans *Microsoft Windows*** (se référer à ce bulletin pour obtenir les informations techniques nécessaires à la mise en œuvre de cette mesure).

  Le correctif s'applique sur l'ensemble des systèmes d'exploitation *Microsoft Windows 10, Windows Server 2016* et *Windows Server 2019* présents sur le parc informatique.

- **CERTFR-2020-ALE-005** (www.cert.ssi.gouv.fr/alerte/CERTFR-2020-ALE-005) – **Multiples vulnérabilités dans le serveur de passerelle RDP de Windows** (se référer à ce bulletin pour obtenir les informations techniques nécessaires à la mise en œuvre de cette mesure)

  Le correctif s'applique sur l'ensemble des systèmes d'exploitation *Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019.*

  En ce qui concerne les produits Citrix ADC, Citrix Gateway et Citrix SD-WAN WANOP des correctifs, qu'il conviendra d'appliquer, seront publiés les 20, 27 et 31 janvier. Des mesures de contournement provisoires ont par ailleurs été proposées :

- **CERTFR-2020-ALE-002** (www.cert.ssi.gouv.fr/alerte/CERTFR-2020-ALE-002) – **Vulnérabilité dans les produits Citrix ADC et Citrix Gateway** (se référer à ce bulletin pour obtenir les informations techniques nécessaires à la mise en œuvre des mesures de contournements)

Les autres mesures activées du domaine de la sécurité du numérique restent inchangées.