Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

S . G . D . S . N
Agence nationale
de la sécurité des
systèmes d'information

Paris, le 18 mars 2020
N° CERTFR-2020-ACT-002

Affaire suivie par: CERT-FR

BULLETIN D'ACTUALITÉ DU CERT-FR

Objet: Bulletin d'actualité CERTFR-2020-ACT-002

Gestion du document

Référence	CERTFR-2020-ACT-002
Titre	Bulletin d'actualité CERTFR-2020-ACT-002
Date de la première version	18 mars 2020
Date de la dernière version	18 mars 2020
Source(s)	Alerte CERTFR-2020-ALE-008 du 11 mars 2020 Alerte CERTFR-2020-ALE-007 du 27 février 2020
Pièce(s) jointe(s)	Aucune(s)

Tableau 1: Gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

Télé-travail : Protégez vos Systèmes d'Information

Contexte

Pour faire face à la crise sanitaire actuelle, le gouvernement demande à tous de télétravailler dès lors que cela est possible. La mise en œuvre de cette mesure nécessite pour beaucoup d'employeurs de mettre en œuvre ou de renforcer des moyens de télétravail dans l'urgence.

Ces moyens d'accès à distance augmentent l'exposition des systèmes d'information (SI) sur Internet, dans un contexte où les risques pour leur sécurité sont très élevés (cf. [1] et [2] notamment) avec les découvertes récentes de vulnérabilités critiques touchant certaines de ces solutions (cf. [3], [4], [5], [6], [7] et [8] par exemple).

Enfin, un grand nombre de fraudes se développent qui peuvent notamment affecter les personnes en situation de télétravail. Il est nécessaire de sensibiliser ses équipes à ces risques qui peuvent les affecter à titre professionnel, mais également personnel[9].

Systèmes affectés

Tout système d'information (SI), qu'il s'agisse d'un SI interne ou d'un SI hébergé en nuage (*Cloud* public ou privé) disposant d'une solution d'accès à distance en mode 'nomadisme'.

Recommandations

Les objectifs de ce bulletin sont de rappeler les bonnes pratiques à respecter pour limiter les risques pour la sécurité des systèmes d'information et d'expliciter les comportements à bannir.

Compte tenu de l'actualité, il est important de n'**exposer sous aucun prétexte sur Internet** les interfaces web de serveurs ***Microsoft Exchange*** qui ne sont pas au dernier niveau de correctif. Comme explicité dans le dernier bulletin d'alerte associé [3], les codes d'exploitation sont publics et des attaques sont en cours en ce moment même. Il est également important de ne pas donner un accès à vos serveurs de partage de fichiers via le protocole SMB [4].

De manière générale, si vous exposez ou devez impérativement exposer de nouveaux services sur Internet, **mettez les à jour au plus vite** avec les derniers correctifs de sécurité et activez les mécanismes de journalisation. Dans la mesure du possible, activez l'authentification double facteur.

Pour conclure, les bonnes pratiques suivantes contribuent à limiter les risques pour les systèmes d'information :

- Appliquer les correctifs de sécurité rapidement, notamment sur les équipements et logiciels exposés sur Internet (solution VPN, solution de bureau distant, solution de messagerie, etc.) ;
- Effectuer des sauvegardes hors ligne pour vos systèmes critiques ;
- Utiliser une solution d'accès de type VPN (*Virtual Private Network*, réseau privé virtuel) propre à l'entreprise, idéalement IPsec ou TLS à défaut, pour ne pas exposer les applications directement sur Internet ;
- Mettre en œuvre des mécanismes d'authentification à double facteur pour limiter les risques d'usurpation d'identité (VPN et applications accessibles) ;
- Consulter régulièrement les journaux d'accès aux solutions exposées sur Internet pour détecter des comportements suspects.

Le bulletin du CERT-FR [10] référence notamment le guide nomadisme [11].

Documentation

- [1] https://www.cert.ssi.gouv.fr/cti/CERTFR-2020-CTI-002/
- [2] https://www.cert.ssi.gouv.fr/cti/CERTFR-2020-CTI-001/
- [3] correctif de sécurité pour Microsoft Exchange : https://www.cert.ssi.gouv.fr/alerte/CERTFR-2020-ALE-007/
- [4] correctif de sécurité pour le protocole de partage de fichier SMB de Microsoft : https://www.cert.ssi.gouv.fr/alerte/CERTFR-2020-ALE-008/

- [5] correctif de sécurité pour Remote Desktop Gateway : https://www.cert.ssi.gouv.fr/alerte/CERTFR-2020-ALE-005/
- [6] correctif de sécurité pour Citrix Gateway et Citrix ADC : https://www.cert.ssi.gouv.fr/alerte/CERTFR-2020-ALE-002/
- [7] correctif de sécurité pour Microsoft Sharepoint : https://www.cert.ssi.gouv.fr/alerte/CERTFR-2019-ALE-008/
- [8] correctif de sécurité pour les VPN : https://www.cert.ssi.gouv.fr/alerte/CERTFR-2020-ALE-001/ et https://www.cert.ssi.gouv.fr/actualite/CERTFR-2019-ACT-008/
- [9] https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/coronavirus-covid-19-vigilance-cybersecurite
- [10] https://www.cert.ssi.gouv.fr/actualite/CERTFR-2020-ACT-001/
- [11] https://www.ssi.gouv.fr/nomadisme-numerique

Rappel des avis émis

Dans la période du 09 au 15 mars 2020, le CERT-FR a émis les publications suivantes :

- CERTFR-2020-ALE-008 : Vulnérabilité dans l'implémentation du protocole SMB par Microsoft
- CERTFR-2020-AVI-131 : Multiples vulnérabilités dans Google Chrome OS
- CERTFR-2020-AVI-132 : [SCADA] Multiples vulnérabilités dans les produits Siemens
- CERTFR-2020-AVI-133 : Multiples vulnérabilités dans Microsoft IE
- CERTFR-2020-AVI-134 : Multiples vulnérabilités dans Microsoft Edge
- CERTFR-2020-AVI-135 : Multiples vulnérabilités dans Microsoft Office
- CERTFR-2020-AVI-136 : Multiples vulnérabilités dans Microsoft Windows
- CERTFR-2020-AVI-137 : Multiples vulnérabilités dans les produits Microsoft
- CERTFR-2020-AVI-138 : Multiples vulnérabilités dans Mozilla Firefox
- CERTFR-2020-AVI-139 : Multiples vulnérabilités dans les produits Intel
- CERTFR-2020-AVI-140 : Multiples vulnérabilités dans les produits SAP
- CERTFR-2020-AVI-141 : Vulnérabilité dans GitLab
- CERTFR-2020-AVI-142 : Multiples vulnérabilités dans Palo Alto PAN-OS
- CERTFR-2020-AVI-143 : [SCADA] Multiples vulnérabilités dans les produits Schneider Electric
- CERTFR-2020-AVI-144 : Vulnérabilité dans Xen
- CERTFR-2020-AVI-145 : Multiples vulnérabilités dans Joomla!
- CERTFR-2020-AVI-146 : Multiples vulnérabilités dans les produits Fortinet
- CERTFR-2020-AVI-147 : Multiples vulnérabilités dans le noyau Linux de Red Hat
- CERTFR-2020-AVI-148 : Multiples vulnérabilités dans le noyau Linux de SUSE
- CERTFR-2020-AVI-149 : Vulnérabilité dans implémentation du protocole SMB par Microsoft
- CERTFR-2020-AVI-150 : Multiples vulnérabilités dans les produits VMware
- CERTFR-2020-AVI-151 : Vulnérabilité dans Belden HiOS et HiSecOS

Gestion détaillée du document

le 18 mars 2020
Version initiale