Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 26 septembre 2016
N° CERTFR-2016-ACT-039

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2016-ACT-039

1 - Mise en garde concernant l'utilisation du protocole SMBv1

Le bulletin d'actualité CERTFR-2016-ACT-038 ainsi que l'avis CERTFR-2016-AVI-310 faisait mention d'une vulnérabilité dans le protocole *Service Message Block* (SMB) v1.0 . Cette version du protocole est relativement ancienne et devrait être désactivée.

Historique

Le protocole *Service Message Block* (SMB), souvent connu sous le sigle CIFS (*Common Internet File System*), a été popularisé par le système d'exploitation Microsoft Windows, puisqu'étant par défaut celui utilisé pour le partage de fichiers.

Ce protocole a connu plusieurs évolutions majeures, notamment en 2006 (avec les systèmes Windows Vista et Server 2008) pour la version 2.0 et en 2012 (avec Windows 8 et Windows Server 2012) pour la version 3.0.

Sécurité

La première version de ce protocole est relativement ancienne et source d'un certain nombre de défauts relatifs à la sécurité. En premier lieu, la signature des messages implémentée dans SMB v1.0 fait appel à la fonction de hachage MD5, considérée comme obsolète. Les versions 2.02 et 3.0 changent cette valeur pour des fonctions de hachage plus robustes (HMAC SHA-256 et AES-CMAC).

D'autre part, la version 3.0 de SMB apporte le support du chiffrement. Les versions précédentes ne supportant pas cette fonctionnalité, il est possible pour un attaquant d'intercepter l'ensemble des documents transitant sur le réseau de l'entreprise par le biais d'une attaque de l'homme du milieu.

Enfin, les systèmes d'exploitation Microsoft supportant uniquement la version 1.0 de ce protocole, soit Windows XP et Windows Server 2003, ne sont plus supportés par l'éditeur et ne devraient par conséquent plus être en production. Les versions ultérieures de ces systèmes d'exploitation supportent quant à eux à minima SMB v2.0.

Audit de l'utilisation de SMB v1.0

Afin de déterminer le taux d'utilisation de SMB v1.0 et évaluer l'impact d'une désactivation de cette version sur le réseau, il existe une commande permettant d'auditer l'utilisation de ce protocole (disponible sur les systèmes Windows 10 et Server 2016) en générant des journaux d'évènements :

```
Set-SmbServerConfiguration -AuditSmb1Access $true
```

Recommandations

Le CERT-FR recommande :

- de désactiver le support du protocole SMBv1 sur les versions supérieures ou égales à Windows 7 et Windows Server 2008 ;
- de migrer et décommissionner les versions obsolètes et non supportées des systèmes d'exploitation dans l'entreprise ;
- de maintenir les systèmes serveurs et client à jour en appliquant régulièrement les correctifs de sécurité.

Documentation

- https://support.microsoft.com/fr-fr/kb/2696547
- https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/

2 - Rappel des avis émis

Dans la période du 19 au 25 septembre 2016, le CERT-FR a émis les publications suivantes :

- CERTFR-2016-ALE-007 : Vulnérabilité dans Cisco IOS, IOS EX et IOS XR
- CERTFR-2016-AVI-315 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu
- CERTFR-2016-AVI-316 : Multiples vulnérabilités dans les produits Apple
- CERTFR-2016-AVI-317 : Multiples vulnérabilités dans Mozilla Firefox
- CERTFR-2016-AVI-318 : Multiples vulnérabilités dans les produits Cisco
- CERTFR-2016-AVI-319 : Multiples vulnérabilités dans Drupal
- CERTFR-2016-AVI-320 : Multiples vulnérabilités dans OpenSSL

Gestion détaillée du document

26 septembre 2016 version initiale.