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 03 juillet 2017
N° CERTFR-2017-ACT-026

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2017-ACT-026

1 - Sensibilisation sur les serveurs FTP avec accès anonyme

A la suite de nombreux signalements, le CERT-FR a récemment constaté une recrudescence de services FTP accessibles anonymement sur Internet. Ces accès peuvent être utilisés à des fins malveillantes et il convient de les protéger.

Contexte

Le protocole FTP (*File Transfer Protocol*) est communément utilisé sur Internet et dans les réseaux d'entreprise pour le transfert de fichiers. Il peut être souvent rencontré lorsqu'il s'agit d'alimenter un site Web chez un hébergeur.

La plupart des logiciels de type "serveur FTP" sont souvent configurés par défaut pour autoriser les accès anonymes en lecture, voire aussi en écriture. Cela signifie que le contenu hébergé par ce serveur est accessible via ce protocole avec le couple nom d'utilisateur / mot de passe suivant : *anonymous / (mot de passe vide)*.

Lorsque ce type de configuration est rencontré, un attaquant peut lister l'ensemble des données hébergées par ce service voire même, lorsque l'accès en écriture est autorisé pour le compte *anonymous*, altérer ou supprimer le contenu présent sur le serveur. Ce même attaquant peut également héberger du contenu malveillant et/ou illicite sur ce serveur.

Il est également à noter que certains moteurs de recherche spécialisés (tels que *Shodan*) permettent facilement de lister des serveurs présentant ce type de configuration.

Sécurité

Afin de limiter les risques, il convient de désactiver l'accès anonyme aux services FTP et d'activer des accès spécifiques pour chaque utilisateur du service. Il est également recommandé de ne pas publier de documents sensibles sur ce type de service.

Enfin, de part sa construction, les informations transportées au travers du protocole FTP transitent en clair sur le réseau. Ce mode de fonctionnement permet à un attaquant d'intercepter et de modifier le contenu des données transitant via ce protocole. Dès lors, il conviendra d'utiliser le protocole FTPS (*File Transfer Protocol Secure*), reposant sur TLS (*Transport Layer Security*), afin de protéger les données. SFTP (*SSH File Transfer Protocol*), reposant sur SSH, peut également être une alternative.

Recommandations

Le CERT-FR recommande :

- de désactiver les accès anonymes sur les services FTP, notamment ceux exposés sur Internet ;
- de désactiver les services FTP lorsque ceux-ci sont inutilisés ;
- de ne pas publier de documents sensibles sur les services exposés sur Internet ;

- de maintenir les systèmes serveurs et clients à jour en appliquant régulièrement les correctifs de sécurité ;
- d'effectuer des sauvegardes régulières des données hébergées par ces services ;
- d'utiliser une politique de mots de passe robustes pour les accès aux services ;
- d'activer la journalisation sur les services FTP ;
- d'activer le chiffrement (en passant par les protocoles SFTP ou FTPS par exemple) afin de sécuriser les communications.

2 - Rappel des avis émis

Dans la période du 19 juin au 02 juillet 2017, le CERT-FR a émis les publications suivantes :

- CERTFR-2017-ALE-012 : Campagne de maliciels prenant l'apparence d'un rançongiciel à multiples capacités de propagation
- CERTFR-2017-AVI-185 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu
- CERTFR-2017-AVI-186 : Multiples vulnérabilités dans Oracle Solaris
- CERTFR-2017-AVI-187 : Multiples vulnérabilités dans le noyau Linux de RedHat
- CERTFR-2017-AVI-188 : Multiples vulnérabilités dans le noyau Linux de SUSE
- CERTFR-2017-AVI-189 : Vulnérabilité dans SCADA Siemens SIMATIC CP 44x-1 RNA modules
- CERTFR-2017-AVI-190 : Multiples vulnérabilités dans Xen
- CERTFR-2017-AVI-191 : Multiples vulnérabilités dans les produits Cisco
- CERTFR-2017-AVI-192 : Multiples vulnérabilités dans Drupal
- CERTFR-2017-AVI-193 : Vulnérabilité dans SCADA Siemens XHQ
- CERTFR-2017-AVI-194 : Multiples vulnérabilités dans les produits Microsoft
- CERTFR-2017-AVI-195 : Multiples vulnérabilités dans Citrix XenServer
- CERTFR-2017-AVI-196 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu
- CERTFR-2017-INF-001 : Protection contre les rançongiciels

Gestion détaillée du document

03 juillet 2017 version initiale.