

Groupe de travail Réseau
Request for Comments : 2577
Catégorie : Information
Traduction Claude Brière de L'Isle

M. Allman, NASA Glenn/Sterling Software
S. Ostermann, Ohio University
mai 1999

Considérations sur la sécurité de FTP

Statut de ce mémoire

Le présent mémoire apporte des informations pour la communauté de l'Internet. Il ne spécifie aucune norme de l'Internet. La distribution du présent mémoire n'est soumise à aucune restriction.

Notice de copyright

Copyright (C) The Internet Society (1999). Tous droits réservés.

Résumé

La spécification du protocole de transfert de fichiers (FTP, *File Transfer Protocol*) contient un certain nombre de mécanismes qui peuvent être utilisés pour compromettre la sécurité du réseau. La spécification FTP permet à un client de donner ordre à un serveur de transférer des fichiers à une machine tierce. Ce mécanisme de tiers, appelé un mandataire FTP, cause un problème de sécurité bien connu. La spécification FTP permet aussi un nombre illimité de tentatives d'entrée du mot de passe d'un usager. Cela permet les attaques en force brute pour "deviner un mot de passe". Le présent document donne des suggestions pour que les administrateurs de système et ceux qui mettent en œuvre les serveurs FTP puissent diminuer les problèmes de sécurité associés à FTP.

1. Introduction

La spécification du protocole de transfert de fichier (FTP) [RFC959] fournit un mécanisme qui permet à un client d'établir une connexion de contrôle FTP et de transférer un fichier entre deux serveurs FTP. Ce mécanisme de "mandataire FTP" peut être utilisé pour diminuer la quantité de trafic sur le réseau ; le client ordonne à un serveur de transférer un fichier à un autre serveur, plutôt que de transférer le fichier du premier serveur au client puis du client au second serveur. Ceci est particulièrement utile lorsque le client se connecte au réseau en utilisant une liaison lente (par exemple, un modem). Bien qu'utile, le mandataire FTP pose un problème de sécurité qu'on appelle une "attaque de rebond" [CERT97:27]. En plus de l'attaque de rebond, les serveurs FTP peuvent être utilisés par des attaquants pour deviner les mots de passe en utilisant la force brute.

Le présent document ne comporte pas une discussion de FTP lorsque utilisé en conjonction avec de forts protocoles de sécurité, tels que la sécurité IP. Ces soucis de sécurité devraient être documentés, ils sont cependant en dehors du domaine d'application du présent document.

Le présent article donne des informations pour les mises en œuvre de serveur FTP et les administrateurs de système, comme suit. La Section 2 décrit une "attaque de rebond" FTP. La Section 3 fait des suggestions pour minimiser l'attaque de rebond. La Section 4 fait des suggestions pour les serveurs qui limitent l'accès sur la base de l'adresse réseau. La Section 5 fait des recommandations pour limiter les tentatives de "deviner le mot de passe" en force brute par des clients. Ensuite, la Section 6 fait une brève discussion des mécanismes pour améliorer la confidentialité. La Section 7 fournit un mécanisme pour empêcher de deviner l'identité de l'usager. La Section 8 discute de la pratique du vol d'accès. Finalement, la Section 9 fait un survol des autres questions de sécurité de FTP en rapport avec les bogues logicielles plutôt que des problèmes de protocole.

2. L'attaque du rebond

La version du protocole FTP spécifiée dans la norme [RFC959] fournit une méthode pour attaquer les serveurs bien connus du réseau, tout en rendant leurs auteurs difficiles à débusquer. L'attaque implique l'envoi d'une commande FTP "PORT" à un serveur FTP contenant l'adresse réseau et le numéro d'accès de la machine et du service attaqués. À ce point, le client d'origine peut ordonner au serveur FTP d'envoyer un fichier au service qui est attaqué. Un tel fichier va contenir des commandes pertinentes pour le service attaqué (SMTP, NNTP, etc.). Ordonner à un tiers de se connecter au service, plutôt que de se connecter directement, rendant le traçage de l'agresseur difficile et peut circonvenir les restrictions d'accès fondées sur l'adresse réseau.

Par exemple, un client télécharge un fichier contenant des commandes SMTP à un serveur FTP. Puis, utilisant une commande PORT appropriée, le client ordonne au serveur d'ouvrir une connexion avec l'accès SMTP d'une machine tierce. Finalement, le client ordonne au serveur de transférer le fichier téléchargé contenant les commandes SMTP à la machine tierce. Cela peut permettre au client de falsifier la messagerie sur la machine tierce sans faire une connexion directe. Cela rend difficile la traque des attaquants.

3. Protection contre l'attaque de rebond

La spécification FTP d'origine [RFC959] suppose que les connexions de données seront faites en utilisant le protocole de contrôle de transmission (TCP) [RFC793]. Les numéros d'accès TCP dans la gamme de 0 à 1023 sont réservés pour les services bien connus tels que la messagerie, les nouvelles du réseau et les connexions de contrôle FTP [RFC1700]. La spécification FTP ne fait aucune restriction sur les numéros d'accès TCP utilisés pour la connexion de données. Donc, en utilisant un mandataire FTP, les clients ont la capacité de dire au serveur d'attaquer un service bien connu sur n'importe quelle machine.

Pour éviter de telles attaques de rebond, il est suggéré que les serveurs n'ouvrent pas de connexions de données avec les accès TCP inférieurs à 1024. Si un serveur reçoit une commande PORT contenant un numéro d'accès TCP inférieur à 1024, la réponse suggérée est 504 (définie comme "Commande non mise en œuvre pour ce paramètre" par la [RFC959]). Noter que cela laisse quand même les serveurs non bien connus (ceux qui fonctionnent sur les accès supérieurs à 1023) vulnérables aux attaques de rebond.

Plusieurs propositions (par exemple, les [RFC1639] et [RFC2428]) fournissent un mécanisme qui permettrait d'établir des connexions en utilisant un protocole de transport autre que TCP. Des précautions similaires devraient être prises pour protéger les services bien connus lors de l'utilisation de ces protocoles.

Noter aussi que l'attaque de rebond exige généralement qu'un attaquant soit capable de télécharger un fichier sur un serveur FTP et ensuite de le transporter jusqu'au service attaqué. Utiliser les protections de fichier appropriées empêchera ce comportement. Cependant, les attaquants peuvent aussi attaquer des services en envoyant des données aléatoires à partir d'un serveur FTP distant, ce qui peut causer des problèmes à certains services.

Désactiver la commande PORT est aussi une option pour se protéger contre l'attaque de rebond. La plupart des transferts de fichiers peuvent être faits en utilisant seulement la commande PASV [RFC1579]. L'inconvénient de désactiver la commande PORT est qu'on perd la capacité à utiliser un mandataire FTP, mais les mandataires FTP peuvent n'être pas nécessaires dans un certain environnement.

4. Restriction d'accès

Pour certains serveurs FTP, il est souhaitable de restreindre l'accès sur la base de l'adresse réseau. Par exemple, un serveur peut vouloir restreindre l'accès à certains fichiers à partir de certains endroits (par exemple, un certain fichier ne devrait pas être transféré en dehors d'une organisation). Dans une telle situation, le serveur devrait confirmer que l'adresse réseau des hôtes distants à la fois sur la connexion de contrôle et sur la connexion de données sont à l'intérieur de l'organisation avant d'envoyer un fichier soumis à ces restrictions. En vérifiant les deux connexions, un serveur se protège contre le cas où la connexion de contrôle est établie avec un hôte de confiance et où la connexion de données ne l'est pas. De même, le client devrait vérifier l'adresse IP de l'hôte distant après l'acceptation d'une connexion sur un accès ouvert en mode d'écoute, pour vérifier que la connexion a été faite par le serveur prévu.

Noter que restreindre l'accès sur la base de l'adresse réseau laisse le serveur FTP vulnérable aux attaques par "usurpation". Dans une attaque par usurpation, par exemple, la machine attaquante pourrait deviner l'adresse d'hôte de l'autre machine à l'intérieur d'une organisation et télécharger des fichiers qui ne sont pas accessibles de l'extérieur de l'organisation. Chaque fois que possible, un mécanisme sûr d'authentification devrait être utilisé, comme ceux mentionnés dans la [RFC2228].

5. Protection des mots de passe

Pour minimiser le risque que le mot de passe soit deviné par une attaque en force brute à travers le serveur FTP, il est suggéré que les serveurs limitent le nombre de tentatives qui peuvent être faites pour l'envoi du mot de passe correct. Après un petit nombre de tentatives (3 à 5), le serveur devrait clore la connexion de contrôle avec le client. Avant de clore la connexion de contrôle, le serveur doit envoyer au client un code de retour de 421 ("Service non disponible, clôture de la connexion de contrôle" [RFC959]). Il est de plus suggéré que le serveur impose un délai de 5 secondes avant de répondre à

une commande "PASS" invalide pour diminuer l'efficacité d'une attaque en force brute. S'il en est de disponible, les mécanismes déjà fournis par le système d'exploitation cible devraient être utilisés pour mettre en œuvre ces suggestions.

Un intrus peut subvertir les mécanismes ci-dessus en établissant plusieurs connexions de contrôle en parallèle avec un serveur. Pour combattre l'utilisation de connexions concurrentes multiples, le serveur pourrait soit limiter le nombre total de connexions de contrôle possibles, soit tenter de détecter les activités suspectes à travers les sessions et refuser d'autres connexions à partir du site. Cependant, ces deux mécanismes ouvrent la porte à des attaques de "déli de service", dans lesquelles l'attaquant initie délibérément l'attaque pour priver d'accès un utilisateur valide.

La norme FTP [RFC959] envoie les mots de passe en clair en utilisant la commande "PASS". Il est suggéré que les clients et serveurs FTP utilisent d'autres mécanismes d'authentification qui ne soient pas sujets à l'espionnage (comme le mécanisme développé par le groupe de travail Technologies d'authentification courantes de l'IETF [RFC2228]).

6. Confidentialité

Toutes les informations de données et de contrôle (y compris les mots de passe) sont envoyées sous forme non chiffrée à travers le réseau par le FTP standard [RFC959]. Pour garantir la confidentialité des informations que transmet FTP, un schéma de chiffrement fort devrait être utilisé chaque fois que possible. Un tel mécanisme est défini dans la [RFC2228].

7. Protection des noms d'utilisateur

La norme FTP [RFC959] spécifie une réponse 530 à la commande USER lorsque le nom d'utilisateur est rejeté. Si le nom d'utilisateur est valide et qu'un mot de passe est exigé, FTP retourne à la place une réponse 331. Pour empêcher un client malveillant de déterminer des noms d'utilisateurs valides sur un serveur, il est suggéré qu'un serveur retourne toujours 331 à la commande USER puis rejette ensuite la combinaison de nom d'utilisateur et mot de passe pour un nom d'utilisateur invalide.

8. Vol d'accès

De nombreux systèmes d'exploitation allouent des numéros d'accès dynamiques en ordre croissant. En faisant un transfert légitime, un attaquant peut observer le numéro d'accès actuellement alloué par le serveur et "deviner" quel est le prochain qui sera utilisé. L'attaquant peut faire une connexion à cet accès, puis dénier à un autre client légitime la capacité à effectuer un transfert. Autrement, l'attaquant peut voler un fichier destiné à un utilisateur légitime. De plus, un attaquant peut insérer un fichier falsifié dans le flux de données et le faire passer comme venant d'un client authentifié. Ce problème peut être atténué en faisant que clients et serveurs FTP utilisent des numéros d'accès local aléatoires pour les connexions de données, soit en exigeant des accès aléatoires du système d'exploitation, soit en utilisant des mécanismes dépendants du système.

9. Problèmes de sécurité fondés sur le logiciel

Le présent document met l'accent sur les problèmes de sécurité en relation avec le protocole. Il y a un certain nombre de problèmes en rapport avec la sécurité de FTP qui sont documentés et sont dus à une mauvaise mise en œuvre. Bien que les détails de ces types de problèmes sortent du domaine d'application du présent document, on doit mentionner que les dispositifs FTP suivants ont été victimes d'abus dans le passé et devraient être traités avec une grande attention par les futures mises en œuvre :

FTP anonyme

FTP anonyme se réfère à la capacité d'un client de se connecter à un serveur FTP avec une authentification minimale et d'obtenir l'accès à des fichiers publics. Des problèmes de sécurité surviennent lorsque un tel utilisateur peut lire tous les fichiers, ou peut créer des fichiers, sur le système [CERT92:09], [CERT93:06].

Exécution de commande à distance

Une extension facultative à FTP, "SITE EXEC", permet aux clients d'exécuter des commandes arbitraires sur le serveur. Ce dispositif devrait évidemment être mis en œuvre avec de grandes précautions. Il y a plusieurs cas documentés d'utilisation de la commande FTP "SITE EXEC" pour subvertir la sécurité d'un serveur [CERT94:08], [CERT95:16].

Code de débogage

Plusieurs cas de compromission de la sécurité se rapportant à FTP peuvent être attribués à un logiciel installé avec des facilités de débogage activées [CERT88:01].

Le présent document recommande que les mises en œuvre de serveurs FTP qui ont ces capacités revoient tous les conseils du CERT sur les attaques sur ces mécanismes ou des mécanismes similaires avant de publier leur logiciel.

10. Conclusion

Utiliser les suggestions ci-dessus peut diminuer les problèmes de sécurité associés aux serveurs FTP sans éliminer de fonctionnalités.

11. Considérations pour la sécurité

Les questions de sécurité sont discutées tout au long de ce mémoire.

Remerciements

Nous tenons à remercier Alex Belits, Jim Bound, William Curtin, Robert Elz, Paul Hethmon, Alun Jones et Stephen Tihor de leurs utiles commentaires sur le présent article. Nous remercions aussi les membres du groupe de travail FTPEXT qui ont fait de nombreuses suggestions utiles à la réunion de Memphis de l'IETF.

Références

- [CERT88:01] CERT Advisory CA-88:01. ftpd Vulnerability. décembre 1988, à ftp://info.cert.org/pub/cert_advisories/
- [CERT92:09] CERT Advisory CA-92:09. AIX Anonymous FTP Vulnerability. 27 avril 1992, à ftp://info.cert.org/pub/cert_advisories/
- [CERT93:06] CERT Advisory CA-93:06. Wuarchive ftpd Vulnerability. 19 septembre 1997, à ftp://info.cert.org/pub/cert_advisories/
- [CERT94:08] CERT Advisory CA-94:08. ftpd Vulnerabilities. 23 septembre 1997, à ftp://info.cert.org/pub/cert_advisories/
- [CERT95:16] CERT Advisory CA-95:16. wu-ftp Misconfiguration Vulnerability. 23 septembre 1997, à ftp://info.cert.org/pub/cert_advisories/
- [CERT97:27] CERT Advisory CA-97.27. FTP Bounce. 8 janvier 1998, à ftp://info.cert.org/pub/cert_advisories/
- [RFC0793] J. Postel (éd.), "Protocole de [commande de transmission](#) – Spécification du protocole du programme Internet DARPA", STD 7, septembre 1981.
- [RFC0959] J. Postel et J. Reynolds, "Protocole de [transfert de fichiers](#) (FTP)", STD 9, octobre 1985. (MàJ par [RFC7151](#))
- [RFC1579] S. Bellovin, "Pare-feu FTP facile", février 1994. (*Information*)
- [RFC1639] D. Piscitello, "Fonctionnement de FTP sur les [gros enregistrements d'adresse](#) (FOOBAR)", juin 1994. (*Exp.*)
- [RFC1700] J. Reynolds et J. Postel, "[Numéros alloués](#)", STD 2, octobre 1994. (*Historique, voir www.iana.org*)
- [RFC2228] M. Horowitz, S. Lunt, "[Extensions de sécurité pour FTP](#)", octobre 1997. (*P.S.*)
- [RFC2428] M. Allman, S. Ostermann, C. Metz, "[Extensions de FTP](#) pour IPv6 et les NAT", septembre 1998. (*P.S.*)

Adresse des auteurs

Mark Allman
NASA Glenn Research Center/Sterling Software
21000 Brookpark Rd. MS 54-2
Cleveland, OH 44135
USA
mél : mallman@grc.nasa.gov

Shawn Ostermann
School of Electrical Engineering and Computer Science
Ohio University
416 Morton Hall
Athens, OH 45701
USA
mél : ostermann@cs.ohiou.edu

Déclaration complète de droits de reproduction

Copyright (C) The Internet Society (1999). Tous droits réservés.

Ce document et les traductions de celui-ci peuvent être copiés et diffusés, et les travaux dérivés qui commentent ou expliquent autrement ou aident à sa mise en œuvre peuvent être préparés, copiés, publiés et distribués, partiellement ou en totalité, sans restriction d'aucune sorte, à condition que l'avis de copyright ci-dessus et ce paragraphe soit inclus sur toutes ces copies et œuvres dérivées. Toutefois, ce document lui-même ne peut être modifié en aucune façon, par exemple en supprimant le droit d'auteur ou les références à l'Internet Society ou d'autres organisations Internet, sauf si c'est nécessaire à l'élaboration des normes Internet, auquel cas les procédures pour les droits de reproduction définis dans les processus des normes pour l'Internet doivent être suivies, ou si nécessaire pour le traduire dans des langues autres que l'anglais.

Les permissions limitées accordées ci-dessus sont perpétuelles et ne seront pas révoquées par la Société Internet, ses successeurs ou ayants droit.

Ce document et les renseignements qu'il contient sont fournis "TELS QUELS" et l'INTERNET SOCIETY et l'INTERNET ENGINEERING TASK FORCE déclinent toute garantie, expresse ou implicite, y compris mais sans s'y limiter, toute garantie que l'utilisation de l'information ici présente n'enfreindra aucun droit ou aucune garantie implicite de commercialisation ou d'adaptation à un objet particulier.

Remerciement

Le financement de la fonction d'éditeur des RFC est actuellement fourni par la Internet Society.