Notification simple de nouveaux messages

Network Working Group
Request For Comments : 4146
Catégorie : Informatif

Auteur : R. Gellens - QUALCOMM – Août 2005
Traducteur : N. Schaefer – sN Informatique – Septembre 2005

Statut de ce document

Ce document apporte des informations à la communauté Internet. En aucun cas, ce document ne spécifie pas un standard. La diffusion de ce document est libre.

Copyright

Résumé

Ce document décrit une technique utilisée de longue date, utilisée par un grand nombre de serveurs de messagerie, qui permet aux utilisateurs d'être avertis lors de la réception de nouveaux messages. Les serveurs ne sont pas les seuls à offrir cette fonctionnalité, de nombreux clients la proposent, qu'il s'agisse de clients de messagerie complets ou de clients plus spécialisés dont le rôle est de recevoir les notifications de nouveaux messages afin de prévenir un client de messagerie.

En bref, le serveur envoi la chaîne de caractères « nm_notifyuser » suivie de CRLF au port du protocole finger à l'adresse IP (soit configurée soit la dernière utilisée) de l'utilisateur qui a reçu un nouveau message.

Table des matières

1. Introduction

Il existe une technique utilisée de longue date, utilisée par un grand nombre de serveurs de messagerie, qui permet aux utilisateurs d'êtres avertis lors de la réception de nouveaux messages. Les serveurs ne sont pas les seuls à offrir cette fonctionnalité, de nombreux clients la proposent, qu'il s'agisse de clients de messagerie complets ou de clients plus spécialisés dont le rôle est de recevoir les notifications de nouveaux messages afin de prévenir un client de messagerie. Cette technique est connue sous le nom de « *notify mail* » (due à un logiciel client shareware du même nom), « *biff* », et « *finger hack* ».

2. Conventions utilisées dans ce document

Dans les exemples, « C: » indique les lignes envoyées par le client et « S: » les lignes envoyées le serveur. Les retours à la ligne non représentés par une commande sont uniquement utilisés pour une question de mise en page. Les retours à la ligne présents dans le protocole sont indiqués par « CRLF ».

3. Notification simple de messages

Avec cette technique, le serveur envoi la chaîne de caractères « nm_notifyuser » immédiatement suivie de CRLF au port du protocole finger à l'adresse IP (soit configurée soit la dernière utilisée) de l'utilisateur qui a reçu un nouveau message. Le port utilisé par le protocole finger est le port 79. Notez bien que seul le port du protocole finger est utilisé et en aucun cas le protocole.

L'adresse IP utilisée peut être configurée. Dans le cas contraire le serveur utilisera la dernière adresse IP connue du client, celle qui aura été utilisée lors de la dernière connexion au serveur. Généralement, la configuration de cette option est réglable pour chaque compte.

Sur le système du client, un processus doit écouter sur le port du protocole finger. Lorsqu'il reçoit la chaîne de caractères « nm_notifyuser », une action prédéfinie doit être réalisée, généralement indiquer à un client de messagerie de récupérer les nouveaux messages.

Normalement, une connexion TCP est ouverte vers la cible, le texte « nm_notifyuser » est envoyé, et la connexion est fermée sans attendre de réponse.

Dans certains cas, UDP est utilisé à la place de TCP, mais on utilise généralement le protocole TCP. Même s'il n'y a qu'un seul message envoyé et dans un seul sens (sans réponse), TCP est le protocole le plus utilisé, probablement pour une question de fiabilité.

On suppose que le client qui écoute sur une adresse IP est en charge d'un seul compte de messagerie. Si un client, peut récupérer les messages de plusieurs comptes de messagerie et recevoir le texte « nm_notifyuser », il ne saura pas quel compte est concerné.

Il est bien sûr nécessaire qu'aucun démon finger ne soit actif sur le client.

4. Exemple

Cet exemple indique qu'un nouveau message est arrivé au serveur mail.isp.example.com pour le compte fastness@example.com. Le serveur a déterminé l'adresse IP à laquelle il doit envoyer la notification.

C: <en écoute sur le port 79>
S: <ouverture d'une connexion TCP sur le port 79>
C: <acceptation de la connexion sur le port 79>
S: nm_notifyuser
S: <fermeture de la connexion TCP>

5. Considérations relatives à la sécurité

Il n'y a aucune garantie que le message « nm_notifyuser » est envoyé à la bonne adresse IP. L'agent qui écoute sur le port du client n'a également aucune garantie que le message a été envoyé par un serveur de messagerie qui a reçu un nouveau message pour l'utilisateur.

Il est très simple pour un attaquant d'envoyer un grand nombre de message « nm_notifyuser » à un système pris pour cible. Les clients qui écoutent ce message DOIVENT implémenter un mécanisme de protection contre un envoi massif de messages. De nombreux serveurs disposent déjà de protection contre les utilisateurs qui se connectent et récupèrent leurs courriers électroniques trop souvent.

A cause du fait que ce protocole nécessite l'ouverture d'un port, si l'agent en écoute sur ce port recèle des failles, il peut ouvrir la porte à des attaques distantes (par exemple, le *buffer overflow* qui permet d'exécuter un morceau de code quelconque avec les droits de l'agent). Comme d'habitude, avec un processus

qui écoute sur un port, les droits accordés à ce processus doivent être les plus restreint possibles.

6. Considérations de l’IANA

L’attaque par notification de messages et ce document devraient être pris en compte dans le cadre de l’utilisation du port 79.

7. Remerciements

Le logiciel shareware NotifyMail a été écrit par Scott Gruby.

Coordonnées de l’auteur

Randall Gellens
QUALCOMM Incorporated
6455 Lusk Blvd.
San Diego, CA 92121-2779
USA
Adresse eMail: randy@qualcomm.com

Coordonnées du traducteur

Nils Schaefer
sN Traduction (www.sninformatique.net)
16 rue George Sand
51420 Witry-lès-Reims
France

Téléphone : +33 (03) 26 04 58 65
Adresse email : contact@sninformatique.net