Alerte de Sécurité de Noël : injection php

Mose - 13 Dec 2004 14:08 GMT-0000

A l'attention de tous les développeurs et administrateurs de tikiwikis, ceci est une annonce importante concernant la sécurité des sites Tikiwiki existants, toutes versions confondues. Si vous gérez un Tikiwiki, vous devriez lire attentivement cet article, il contient tous les détails nécessaires à la correction du problème, en une ligne dans un fichier.

Table of contents

Alerte de Sécurité de Noël : injection php

La faille de sécurité

Il n'y avait pas de vérification sur les images téléchargées dans la page d'édition du wiki. Donc un utilisateur mal intentionné disposant de la permission de télécharger des images, pouvait charger un script php et l'appeler directement dans l'arborescence de fichiers, dans le répertoire img/wiki_up. En fait cette faille est plutôt triviale, grossière et évidente. Il est particulièrement étonnant que personne ne l'aie corrigée avant.

Le remède protecteur

Réparez votre tiki dans attendre !

Vérifiez l'integrité de votre tikiwiki

Recherchez dans img/wiki_up/ s'il y a des fichiers avec les extensions .php, .php3, .php4 ou .phtml (ou bien dans img/wiki_up/$tikidomaine dans le cas d'un multitiki). Vous pouvez utiliser les lignes suivantes (en console) pour faciliter votre recherche (fonctionne aussi pour les multitikis)

```
find img/wiki_up -type f -name "*.php" find img/wiki_up -type f -name "*.php3" find img/wiki_up -type f -name "*.php4" find img/wiki_up -type f -name "*.phtml"
```

Vérifiez vos logs apache

Pour savoir si quelqu'un a utilisé cette faille pour injecter un script php malencontreux, vous pouvez 'grepper' vos fichiers de logs apache (si vous pouvez utiliser la commande grep)

```
grep 'img/wiki_up/[^"]*.ph\(p\(3\|4\)\?\|tml\) ' var/log/apache/yourtiki.access.log
```

ou si vous utilisez la rotation de logs et pouvez utiliser zgrep

```
zgrep 'img/wiki_up/[^"]*.ph\(p\(3\|4\)\?\|tml\) ' var/log/apache/yourtiki.access.log*
```

Eliminez le problème

La méthode la plus rapide pour éviter tout problème consiste à désactiver la fonctionnalité "Images" dans le panneau d'administration du wiki (/tiki-admin.php?page=wiki).

Il est égalmement possible de limiter l'usage de cette fonctionnalité en utilisant la permission nommée tiki_p_upload_picture, dans le panneau d'administration des groupes.

Mais le vrai remède, qui permet de continuer à utiliser les images dans les pages wiki, est de mettre à jour ou de modifier le fichier tiki-editpage.php :

- Vous utilisez une version CVS ?
  Mettez à jour votre version, le correctif est présent dans chacune des branches du 1.7 au 1.10
  ```
  cvs -q update -dP
  ```
- Dans le cas contraire (installation avec un .tar.gz)
  Ajouter la ligne suivante dans tiki-editpage.php
  ```
  if (preg_match('/\.(gif|png|jpe?g)$/i',$picname))
  ```
  juste avant la ligne contenant
  ```
  move_uploaded_file( ...
  ```
  - ligne 106 pour la version 1.7.x
  - ligne 138 pour la version 1.8.x
  - lignes 173 et 181 pour la version 1.9rcx
  - ligne 172 pour la version 1.10

La recette du sysadmin

Outre la correction du fichier, vous pouvez également inhiber l'interprétation des fichiers php dans le répertoire img/.

- Si vous utilisez apache, mais n'avez pas accès à sa configuration, créez un fichier .htaccess dans img/wiki_up/ contenant
  ```
  <FilesMatch "\.ph(p(3|4)?|tml)$"> order deny,allow deny from all </FilesMatch>
  ```
  si ca ne marche pas il vous faudra peut-être demander à votre administrateur d'activer cette possibilité d'usage du .htaccess avec
  ```
  AllowOverride Limit
  ```
  dans la directive Directory liées à votre arborescence tiki.

- Si vous pouvez changer votre configuration d'apache, parce que vous l'administrez vous-même, ajoutez
  □□□□□□□□

  ```
  <Directory /var/www/tiki/img> <FilesMatch "\.ph(p(3|4)?|tml)$"> order deny,allow deny from all </FilesMatch> </Directory>
  ```

  en adaptant le chemin pour correspondre à celui du répertoire img/ dans votre installation.

  Les deux méthodes bloqueront simplement l'accès aux fichiers php dans le répertoire img/. Vous pouvez également choisir d'inhiber les fichiers .pl, .vb ou autres si votre configuration globale permet leur interprétation par un autre préprocesseur.

- Pour plus d'informations au sujet de la configuration d'apache consultez http://httpd.apache.org/docs-project/

Nouvelles versions de tikiwiki dans les fourneaux

Pour chaque branche, une nouvelle version de tiki sera publiée dans les jours prochains, sous les versions 1.7.9, 1.8.5 et 1.9dr4. Si vous n'avez pas utilisé l'un des remèdes expliqués plus haut :

vous devriez mettre a jour votre tiki dès que possible.

Gardez en mémoire que vous pouvez toujours alerter le groupe de sécurité de Tikiwiki par l'envoi d'un mail a security at tikiwiki.org (en anglais si possible, sinon en français, il sera compris).

---

mose
pour le tas-de-gens de la sécurité Tikiwiki