

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Problèmes de privilèges dans les extensions de FrontPage

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2000-AVI-011>

Gestion du document

| | |
|-----------------------------|------------------------------------------------------------------------------------------------------|
| Référence | CERTA-2000-AVI-011 |
| Titre | Problèmes de privilèges dans les extensions de FrontPage (FrontPage Server Extensions Ressource Kit) |
| Date de la première version | 27 juin 2000 |
| Date de la dernière version | – |
| Source(s) | Avis K-048 du CIAC |
| Pièce(s) jointe(s) | Aucune |

TAB. 1 – gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

Défiguration de site web.

Le CIAC indique que le risque est élevé, car de multiples pages web ont déjà été défigurées par exploitation des permissions des modules d'extensions de FrontPage (FrontPage Server Extensions Ressource Kit).

2 Systèmes affectés

– Systèmes Unix avec FrontPage Extensions utilisant les serveurs web suivants :

- Apache 1.1.3 ou 1.2
- CERN 3.0
- NCSA 1.5.2
- Netscape Commerce Server 1.12, Communications Server 1.12, Enterprise Server 2.0 et 3.0, FastTrack 2.0
- O'Reilly Website

- Windows NT avec FrontPage Extensions utilisant les serveurs web suivants :
 - Internet Information Server 2.0 ou plus (incluant IIS 4.0)
 - Netscape Commerce Server 1.12, Communications Server 1.12, Enterprise Server 2.0 et 3.0, FastTrack 2.0
 - O'Reilly Website
 - FrontPage Personal Webserver
- Les modules d'extension de FrontPage fonctionnent aussi sous Windows 95 et 98, mais leurs vulnérabilités ne sont pas étudiées ici, car ces systèmes n'ont pas de systèmes de sécurité par le biais de privilèges.

3 Résumé

Les modules d'extensions de FrontPage (Frontpage Server Extensions Ressource Kit) constituent un jeu de programmes permettant la gestion de site web : complément à l'administration du serveur, modifications à distance des pages web et d'autres outils comme, par exemple, le tri des pages web, et suivi de fils de discussions dans les forums etc.

Un administrateur peut rendre, par inadvertance, les modules de gestion de site web de FrontPage exécutables par tous, en changeant les permissions appliquées par défaut aux répertoires d'un site web géré par FrontPage.

4 Description

On peut désigner trois catégories d'utilisateurs des serveurs gérés par FrontPage :

1. les administrateurs qui administrent le serveur web
2. les auteurs (authors) qui créent et modifient les pages web du site
3. les utilisateurs (users) : toute personne susceptible de naviguer sur le site web, y compris l'utilisateur invité IUSR_ si l'accès anonyme est activé.

Les modules d'extension de FrontPage peuvent être installés automatiquement avec Internet Information Server sur un serveur Windows NT. Ils sont aussi utilisés par d'autres gestionnaires de site web tels que Visual InterDev. Une installation automatique rend par défaut les modules inaccessibles à distance, ce qui est le fonctionnement recherché.

Sous Windows NT comme sous Unix, les permissions d'un répertoire peuvent être modifiées de façon récursive, c'est-à-dire que les modifications seront appliquées à tous ses fichiers et sous-répertoires.

Les modules d'extension sont situés dans le répertoire `_vti_bin/`, `_vti_bin/_vti_aut/`, et `_vti_bin/_vti_adm/` installés dans le répertoire racine du serveur web. Ils sont au nombre de trois¹ :

1. `_vti_bin/shtml.dll` qui gère l'interaction entre l'utilisateur consultant le site web et les formulaires HTML. Il doit être accessible par tout utilisateur.
2. `_vti_bin/_vti_adm/admin.dll` commande l'administration du site web, et dont l'accès doit être restreint aux administrateurs du site web.
3. `_vti_bin/_vti_aut/author.dll` qui sert à l'édition distante des pages du site web, et dont l'accès doit être limité aux administrateurs du site ainsi qu'aux seuls auteurs qui ont l'autorisation de modifier les pages de ce site.

Un administrateur du site peut changer par inadvertance les privilèges par défaut de ces répertoires, en changeant de façon récursive les privilèges d'un répertoire parent (situé en amont dans l'arborescence du disque sur lequel ils sont installés).

Il rend alors son serveur vulnérable.

1. Ces trois fichiers ont une extension '.dll' sous Windows NT, ils se termineront par '.exe' et sont situés dans les mêmes répertoire sous Unix

5 Solution

Il faut vérifier et appliquer, si nécessaire, les permissions des répertoires comme suit :

- Sous Windows NT :
 - `_vti_bin` utilisateurs (rx)(rx)², auteurs (rx)(rx), administrateurs (rx)(rx).
 - `_vti_adm` administrateurs (rx)(rx) pas d'accès aux auteurs ou aux utilisateurs.
 - `_vti_aut` auteurs (rx)(rx) administrateurs (rx)(rx) pas d'accès aux utilisateurs
- Sous Unix, c'est à partir du fichier d'accès du serveur³ que FrontPage gère une liste des utilisateurs, groupes et privilèges distincte de celle utilisée par le système, il faut alors modifier les paramètres de ce fichier de la même façon qu'on gère les permissions des scripts ISAPI et CGI⁴ conformément au tableau 2.

| | Administrateur(s) | Auteur(s) | Utilisateurs |
|------------------------------------------------------------|-------------------|-------------|--------------|
| <code>_vti_bin/</code> et <code>shtml.exe</code> | GET, POST | GET POST | GET POST |
| <code>_vti_bin/_vti_adm/</code> et <code>admin.exe</code> | GET, POST | Pas d'accès | Pas d'accès |
| <code>_vti_bin/_vti_aut/</code> et <code>author.exe</code> | GET, POST | GET POST | Pas d'accès |

TAB. 2 – permissions à associer aux modules d'extensions de FrontPage

6 Documentation

- Avis du CIAC :
<http://www.ciac.org/ciac/bulletins/k-048.shtml>
- Documentation de Microsoft sur FrontPage98 Server Extensions Ressource Kit :
<http://officeupdate.microsoft.com/frontpage/wpp/serk98/>
<http://officeupdate.microsoft.com/frontpage/wpp/serk/scintro.htm>

Gestion détaillée du document

27 juin 2000 version initiale.

2. notation pour : (répertoire lisible ainsi que son contenu)(fichiers contenus dans le répertoire lisibles et exécutables)

3. Sous Apache et NCSA : `.htaccess`, sous CERN : `.www_acl`, sous Netscape Server : `.nsconfig`

4. GET : fichier ou répertoire lisible, POST fichier exécutable ou répertoire traversable, et PUT fichier ou répertoire modifiable (ou écrivible). Voir la documentation de FrontPage Server Extensions Ressource Kit, et celle du serveur web utilisé.