Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 08 mars 2013
N° CERTA-2013-ACT-010

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2013-ACT-10

1 Technique d'exploitation PHP

Dans les sites Internet écrits en PHP, une vulnérablité courante est appelée *Local File Inclusion* (LFI). Il s'agit d'une page qui utilise une variable non maîtrisée pour déterminer le chemin d'un second script PHP à exécuter.

Ces vulnérabilités sont généralement considérées comme non critiques, sauf si l'attaquant dispose d'un moyen d'accéder à un fichier dont il contrôle le contenu.

Dans ce cadre, le CERTA a constaté l'utilisation d'une technique d'exploitation où un attaquant exécute un code PHP arbitraire directement depuis une LFI, et peut ainsi compromettre un serveur. Cette technique repose sur l'utilisation d'un champ d'en-tête HTTP contrôlé par le client, qui est passé comme variable d'environnement au script PHP. En incluant le fichier */proc/self/environ*, un fragment de code PHP stocké dans l'en-tête est alors exécuté.

Pour vérifier si vous êtes victime d'une telle tentative de compromission, vous pouvez rechercher l'expression rationnelle suivante sur les fichiers journaux de vos serveurs Web : *grep proc.*environ *.log* .

En cas de résultat positif, il convient de qualifier l'incident, et en cas de compromission avérée, de prendre les mesures appropriées (cf Références).

À noter que cette recherche ne détectera pas les tentatives d'exploitation d'une page qui recevrait ses paramètres via la méthode *POST*.

Afin de prévenir ce type d'attaques, le CERTA recommande d'appliquer les mesures suivantes :

- restreindre les applications Web à un sous-répertoire au niveau du système par l'utilisation d'un *chroot* ;
- durcir la configuration PHP, notamment par l'usage du paramètre *open_basedir* ;
- employer un pare-feu applicatif convenablement configuré.

Documentation

- Que faire en cas de compromission :
  http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-002/

2 Limitation des risques liés à l'accès frauduleux à des pages d'administration de sites Web

Il existe sur l'Internet des bases de données facilement accessibles d'identifiants et de mots de passe par défaut d'accès aux rubriques d'administration de différents gestionnaires de contenu («*CMS*»). Ces bases permettent à un attaquant d'automatiser la recherche de sites mal configurés dont l'interface d'administration est accessible sans

restriction. L'attaquant pourra alors tester les identifiants par défaut, et obtiendra ainsi les privilèges d'administrateur du site, si les mots de passe n'ont pas été modifiés à l'installation du site. Le CERTA profite d'une mise à jour récente de certaines de ces bases pour rappeler quelques recommandations sur la protection de l'accès aux modules d'administration d'un site Web :

- Il est évidemment nécessaire de ne jamais utiliser des identifiants proposés par défaut pour se connecter à une interface d'administration d'un système. Nous recommandons la lecture de la note "Recommandations de Sécurité Relatives aux Mots de passe" du 5 Juin 2012, publiée sur le site de l'ANSSI.
- Les accès aux parties d'administration d'un système depuis l'Internet ne doivent être autorisés que depuis des adresses IP bien identifiées. Ceci permet de se protéger des attaques par dictionnaire automatisées, ainsi que de limiter les dommages causés par le vol des identifiants par un tiers (par exemple via l'utilisation d'enregistreurs de frappes clavier). Cette recommandation s'applique à tout service d'administration (« *Backoffice* » de site Web, accès FTP, SSH, RDP, etc.).
- Lorsque le composant d'administration par le Web ne permet pas de mettre en place ce type de limitation, le serveur Web Apache permet par exemple d'utiliser un fichier *.htaccess* pour restreindre l'accès à une arborescence en fonction de l'adresse IP du visiteur.

Enfin, d'autres recommandations génériques sur la sécurisation de sites Web sont disponibles dans la note d'information CERTA-2012-INF-002 traitant des défigurations de sites Web.

Documentation

- Note Technique *Recommandations de Sécurité Relatives aux Mots de passe*
  http://www.ssi.gouv.fr/IMG/pdf/NP_MDP_NoteTech.pdf
- Tutoriel du serveur HTTP Apache : fichiers .htaccess
  http://httpd.apache.org/docs/2.2/fr/howto/htaccess.html
- Note d'information CERTA-2012-INF-002 : Les défiguration de sites Web
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-INF-002/

3 Sécurité des mots de passe des équipements Cisco

Le CERTA a pu constater des compromissions d'équipements Cisco, en partie dûes à la faiblesse du mode de stockage de leurs mots de passe choisis.

Dans la majorité des équipements Cisco, il existe plusieurs modes qui définissent l'encodage des mots de passe lors du stockage. Avant la version 12.0 de l'IOS, il n'existait que les modes 0 et 7. Le mode 0 conserve le mot de passe en clair tandis que le mode 7 encode le mot de passe avec un algorithme propriétaire réversible de Cisco. Cet algorithme n'apporte cependant aucune protection effective et il existe de nombreux outils disponibles sur l'Internet qui permettent de décoder simplement ces mots de passe.
Depuis la version 12.0, un nouveau mode, le 5, a été introduit. Ce dernier permet d'utiliser l'algorithme MD5 avec une graine pour l'encodage, ce qui améliore considérablement la confidentialité du mot de passe stocké.

Voici un exemple de commande pour créer l'utilisateur "Certa" et le mot de passe associé "t0t01234!" avec le mode 5 :
>username Certa secret 0 t0t01234!
À noter que c'est la commande « secret » qui permet l'utilisation du mode 5. Le 0 permet d'indiquer que le mot de passe entré est en clair mais il sera bien stocké sous forme de condensat MD5.

Le CERTA recommande de veiller à l'utilisation du mode 5 lors de la création de nouveaux mots de passe sur un équipement Cisco et de convertir les mots de passe stockés en mode 0 ou 7 vers le mode 5.

Documentation

- Améliorer la sécurité des mots de passe sur équipement Cisco :
  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/120s_md5.pdf

4 Rappel des avis émis

Dans la période du 01 au 07 mars 2013, le CERTA a émis les publications suivantes :

- CERTA-2013-AVI-159 : Multiples vulnérabilités dans IBM DB2

- CERTA-2013-AVI-160 : Vulnérabilité dans Ubuntu
- CERTA-2013-AVI-161 : Vulnérabilité dans EMC RSA Authentication Agent
- CERTA-2013-AVI-162 : Multiples vulnérabilités dans Google Chrome
- CERTA-2013-AVI-163 : Multiples vulnérabilités dans Oracle Java
- CERTA-2013-AVI-164 : Multiples vulnérabilités dans les produits Apple
- CERTA-2013-AVI-165 : Vulnérabilité dans IBM WebSphere Commerce Enterprise
- CERTA-2013-AVI-166 : Multiples vulnérabilités dans Xerox FreeFlow Print Server
- CERTA-2013-AVI-167 : Multiples vulnérabilités dans MediaWiki
- CERTA-2013-AVI-168 : Multiples vulnérabilités dans TYPO3
- CERTA-2013-AVI-169 : Vulnérabilité dans Citrix Access Gateway Standard Edition
- CERTA-2013-AVI-170 : Vulnérabilité dans le noyau Red Hat

Gestion détaillée du document

08 mars 2013 version initiale.