Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 07 juin 2013
N° CERTA-2013-ACT-023

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2013-ACT-023

1 Vulnérabilité critique dans le CMS SPIP

Une vulnérabilité critique a récemment été détectée et corrigée dans le système de gestion de contenu SPIP, très populaire sur l'Internet. L'exploitation de cette faille logicielle permet à un attaquant d'augmenter ses privilèges sur le site et d'en prendre le contrôle éditorial complet.

Afin de limiter l'exposition aux attaques connues, SPIP propose un mécanisme dit d'écran de sécurité qui permet à la manière d'un pare-feu applicatif, de bloquer les attaques connues et qui pourrait laisser penser que l'application des correctifs de sécurité n'est pas nécessaire.

Le CERTA recommande de n'utiliser ce type de mécanisme de substitution qu'à titre transitoire et de rechercher prioritairement à appliquer les correctifs de sécurité qui sont la seule garantie d'une réelle correction de la vulnérabilité sur les systèmes impactés.

Documentation

– Avis CERTA-2013-AVI-329 :
http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-329/

2 Guide de sécurisation d'*Active Directory*

Microsoft a récemment publié un document détaillé portant sur les bonnes pratiques de sécurité d'un annuaire *Active Directory* (AD), intitulé *Best Practices for Securing Active Directory*. Pour rappel, l'annuaire *Active Directory* doit être un des éléments les plus vigoureusement protégés, car sa compromission est généralement synonyme de compromission *totale* du système d'information d'une organisation.

Ce document est organisé en quatre parties principales :

– les voies menant à une compromission : cette section présente les pratiques d'administration déviantes les plus communément exploitées par les attaquants, de la première intrusion à la compromission totale ;
– la réduction de la surface d'attaque d'*Active Directory* : cette section présente les bonnes pratiques d'administration et de renforcement. Il est notamment proposé une approche de la gestion des groupes et comptes privilégiés qui sont des cibles de choix pour les attaquants ;
– les pistes de surveillance des signes indicateurs d'une compromission : cette section décrit les éléments importants à superviser pour être capable de détecter des tentatives de compromission ;
– l'anticipation de la réponse à une compromission : cette partie contient des recommandations de plus haut niveau visant à se préparer à une compromission. La reconstruction suite à une compromission totale d'un *Active Directory* a en effet plus de chance d'être réussie lorsqu'on y est préparé.

Le document comprend également de nombreux annexes approfondissant certains points ou illustrant la mise en place de recommandations.

Le CERTA recommande la lecture et l'application des recommandations de ce guide.

Documentation

- Annonce de la publication sur le blog de sécurité de Microsoft :
  http://blogs.technet.com/b/security/archive/2013/06/03/microsoft-releases-new-mitigation-guidance-for-active-directory.aspx

3 Rappel des avis émis

Dans la période du 31 mai au 06 juin 2013, le CERTA a émis les publications suivantes :

- CERTA-2013-AVI-335 : Vulnérabilité dans Horde
- CERTA-2013-AVI-336 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu
- CERTA-2013-AVI-337 : Multiples vulnérabilités dans VMware
- CERTA-2013-AVI-338 : Multiples vulnérabilités dans IBM Tivoli Directory Integrator
- CERTA-2013-AVI-339 : Multiples vulnérabilités dans IBM DB2
- CERTA-2013-AVI-340 : Multiples vulnérabilités dans Apple OS X
- CERTA-2013-AVI-341 : Multiples vulnérabilités dans Apple Safari
- CERTA-2013-AVI-342 : Multiples vulnérabilités dans XEN
- CERTA-2013-AVI-343 : Multiples vulnérabilités dans Google Chrome
- CERTA-2013-AVI-344 : Vulnérabilité dans ISC BIND

Gestion détaillée du document

07 juin 2013 version initiale.