Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 25 janvier 2013
N° CERTA-2013-ACT-004

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2013-ACT-004

1 Vulnérabilité critique dans « Joomla! »

Dans le cadre du traitement d'un incident, le CERTA a récemment pu constater l'exploitation d'une vulnérabilité « Joomla! », évoquée dans l'avis CERTA-2012-AVI-152.

Cette vulnérabilité permet une élévation de privilèges lors de la création d'un compte utilisateur. Pour exploiter cette faille, il suffit, lors de la création d'un nouvel utilisateur, d'altérer les données envoyées au serveur en simulant l'appartenance au groupe administrateur. L'attaquant peut ensuite confirmer son inscription et s'identifier, à l'aide de ce nouveau compte, en tant qu'administrateur du site. Il obtient ainsi la possibilité de modifier ou d'ajouter des fichiers sur le serveur. La mise en œuvre de cette vulnérabilité étant particulièrement triviale, elle peut être exploitée sans grande compétence et peut faire l'objet d'un ver.

Les versions de «Joomla!» 2.5.2, 2.5.1, 2.5.0, 1.7.x, 1.6.x sont vulnérables. Il est important de noter que les branches 1.6.x et 1.7.x ne sont plus maintenues et n'auront donc pas de correctif pour cette faille. Afin de corriger cette vulnérabilité, il est donc nécessaire d'effectuer une mise à jour vers la version 2.5.3. Dans le cas d'une impossibilité d'effectuer cette mise à jour, le CERTA recommande de désactiver l'interface permettant la création de nouveaux comptes.

D'une manière plus générale, le CERTA souligne l'importance de tenir à jour les gestionnaires de contenu. En effet, le CERTA a constaté que parmi les attaquants pratiquant la défiguration de sites Internet, beaucoup visent particulièrement ces produits. En effet, les méthodes d'attaques sur ces gestionnaires de contenu sont particulièrement simples et documentées, et des outils d'exploitation sont facilement accessibles.

Documentation

– Avis CERTA-2012-AVI-152 :
http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-152/

2 Détournement de greffons applicatifs (ou plugins)

Le CERTA souhaite attirer l'attention sur un phénomène qui touche les greffons applicatifs (ou *plugins* en anglais). Ces greffons permettent de modifier le comportement d'un logiciel, tel qu'un navigateur ou un client de messagerie, en y ajoutant de nouvelles fonctionnalités ou en changeant le comportement initial du produit.

Des sociétés se spécialisent dans le rachat des greffons populaires afin de pouvoir en acquérir le code et ajouter au produit initial de nouvelles « fonctionnalités », comme l'intégration de publicités ou le suivi de l'activité de l'utilisateur, en vue de pouvoir les monnayer à d'autres entités.

Dans certains cas, afin de respecter les aspects légaux, un paragraphe est ajouté dans les conditions d'utilisation pour informer du comportement particulier, voire intrusif, de l'outil.

Du côté des éditeurs des produits sur lesquels ces greffons sont incorporés, un processus de validation est mis en place pour s'assurer que les greffons qui leur sont soumis sont bien légitimes et ne nuisent pas à l'utilisation de leur produit. Cependant, il est à noter que pour effectuer le transfert de propriété du code source, il n'est pas toujours nécessaire d'en informer l'éditeur. C'est ainsi que les transferts de propriété du code peuvent passer sous le radar de la validation des éditeurs, qui ne seront pas alertés par la publication d'une nouvelle version du greffon.

Le CERTA rappelle que l'utilisation de ces greffons augmente la surface d'attaque d'un logiciel et conseille donc de limiter leur utilisation. Dans le cas où leur utilisation est indispensable, le CERTA recommande de lire attentivement les conditions d'utilisation.

3 Le CERTA et les réseaux sociaux

Il est apparu que certains réseaux sociaux présentent des comptes associés au nom du CERTA.

Ces comptes ne sont pas légitimes. Le CERTA ne communique jusqu'à présent que par le biais de son site Internet et par courrier électronique.

En cas de doute sur une information qui semble provenir du CERTA, n'hésitez pas à nous contacter pour validation.

Documentation

- Page de contact du CERTA :
  http://www.certa.ssi.gouv.fr/certa/contact.html

4 Rappel des avis émis

Dans la période du 18 au 24 janvier 2013, le CERTA a émis les publications suivantes :

- CERTA-2013-AVI-048 : Vulnérabilité dans le système SCADA Schneider Electric SESU
- CERTA-2013-AVI-049 : Multiples vulnérabilités dans Novell eDirectory
- CERTA-2013-AVI-050 : Vulnérabilité dans Foxit Reader
- CERTA-2013-AVI-051 : Vulnérabilité dans IBM Informix
- CERTA-2013-AVI-052 : Multiples vulnérabilités dans Moodle
- CERTA-2013-AVI-053 : Vulnérabilités dans le produit Cisco WRT54GL
- CERTA-2013-AVI-054 : Vulnérabilités dans Avaya Aura Experience Portal
- CERTA-2013-AVI-055 : Vulnérabilités dans EMC AlphaStor
- CERTA-2013-AVI-056 : Vulnérabilité dans Snort
- CERTA-2013-AVI-057 : Vulnérabilité dans EMC Avamar
- CERTA-2013-AVI-058 : Vulnérabilité dans F5 BIG-IP
- CERTA-2013-AVI-059 : Multiples vulnérabilités dans Google Chrome
- CERTA-2013-AVI-060 : Vulnérabilités dans Xen
- CERTA-2013-AVI-061 : Vulnérabilité dans IBM WebSphere
- CERTA-2013-AVI-062 : Multiples vulnérabilités dans Cisco Wireless LAN Controllers

Gestion détaillée du document

25 janvier 2013 version initiale.