Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERT-FR

Paris, le 22 décembre 2014
N° CERTFR-2014-ACT-051

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2014-ACT-051

1 - Vulnérabilité dans les greffons Slider Revolution et Showbiz Pro de Wordpress

Récemment, une vulnérabilité a été découverte dans les greffons WordPress *Slider Revolution* et *Showbiz Pro* [1]. Celle-ci peut être qualifiée de critique puisqu'elle autorise l'inclusion et l'exécution de code PHP arbitraire à distance.

Cette vulnérabilité est massivement exploitée en ce moment. Plus de 11 000 domaines ont été mis en liste noire par Google suite à la compromission de serveurs et leurs utilisations pour distribuer des logiciels malveillants [2].

L'impact de cette vulnérabilité est d'autant plus important que l'utilisation de ces greffons WordPress est très répandue. De nombreux thèmes pour WordPress contiennent l'un ou l'autre de ces greffons, qui peuvent donc être installés à l'insu du webmestre. Le site de vente de greffon Wordpress *Envato Market* a établi une liste des thèmes dans lesquels ces greffons sont présents en précisant les thèmes qui disposent d'une mise à jour de sécurité pour cette vulnérabilité et ceux qui n'en disposent pas encore. [3]

Les tentatives d'exploitation de cette vulnérabilité peuvent être identifiées dans les journaux du serveur web. Un exemple caractéristique d'une attaque débute par la recherche d'une page indiquant la présence des greffons *Slider Revolution* et *Showbiz Pro* :

```
GET /wp-content/plugins/revslider/rs-plugin/font/revicons.eot
```

Si cette page est bien trouvée, les attaquants essaient d'obtenir le fichier `wp-config.php` en exploitant une autre vulnérabilité des greffons. Ce fichier permet de récupérer des informations sur la configuration de base du site web et notamment les identifiants de connexions à la base de données.

```
GET /wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php
```

Les attaquants tentent ensuite d'exploiter la vulnérabilité des greffons leur permettant d'inclure et d'exécuter du code PHP à distance. La requête suivante correspond à l'inclusion du code PHP :

```
POST /wp-admin/admin-ajax.php
```

avec comme données envoyées :

```
Content-Disposition: form-data; revslider_ajax_action
update_plugin; name="update_file"
```

L'attaquant accèdera ensuite au code PHP ainsi inclus (souvent un webshell), par exemple en réalisant une requête sur l'URI :

```
/wp-content/plugins/revslider/temp/update_extract/revslider/update.php
```

Le CERT-FR recommande ainsi de vérifier rapidement si les greffons *Slider Revolution* et *Showbiz Pro* sont utilisés et de les mettre à jour le cas échéant. Dans le cas où la mise à jour n'est pas encore rendue disponible par l'éditeur, ceux-ci peuvent être désactivés.

Si l'un ou l'autre greffon est présent, il convient de vérifier dans les journaux du serveur si des tentatives d'exploitation des vulnérabilités ont eu lieu. En cas d'attaque réussie, le CERT-FR recommande la réinstallation

du site à partir d'une sauvegarde des fichiers et de la base de données réalisées avant l'attaque, ainsi que la mise à jour de l'ensemble des logiciels utilisés.

Documentation

1 http://marketblog.envato.com/news/plugin-vulnerability/

2 http://blog.sucuri.net/2014/12/soaksoak-malware-compromises-100000-wordpress-websites.html

3 http://marketblog.envato.com/news/affected-themes/

2 - Vulnérabilité de type POODLE impactant certaines implémentations logicielles de TLS

Le 16 décembre 2014, la société FireEye a annoncé que certaines implémentations logicielles du protocole TLS étaient vulnérables à une attaque similaire à POODLE. L'attaque POODLE a été rendue publique le 20 octobre 2014 par Google et impacte le protocole SSL 3.0. Cette attaque permet d'accéder en clair à des données échangées de manière sécurisée *via* cette version du protocole SSL.

Rappels sur l'attaque POODLE sur SSL

Le cœur de cette attaque réside dans le fait qu'il est possible dans SSL 3.0 d'écrire ce que l'on souhaite à la fin du message chiffré (sauf le dernier octet). En effet, la fin du message chiffré correspond au *padding* et la seule contrainte imposée par le protocole est que le dernier octet indique la taille de ce *padding*. La possibilité d'écrire arbitrairement le contenu du *padding* permet, *via* une attaque par force brute, de déchiffrer le contenu du message transmis. Jusqu'à maintenant, l'attaque POODLE ne concernait que le protocole SSL 3.0 et ne portait pas sur les implémentations logicielles de TLS, son successeur.

Implémentations TLS concernées par l'attaque

Au niveau du *padding*, la description du protocole TLS impose que la valeur de chacun des octets corresponde à la taille du *padding*. Lors du déchiffrement d'un message chiffré, il convient donc théoriquement de vérifier que tous les octets de *padding* ont bien cette valeur. Or, pour des raisons de performance, certaines implémentations logicielles de TLS (par exemple F5 ou A10) ne vérifient que le premier octet. Dans ce cas, il devient alors possible d'écrire ce que l'on souhaite dans le *padding*, ce qui ouvre la voie à une attaque similaire à POODLE sur SSL 3.0. Néanmoins, le protocole TLS en lui-même reste non affecté. Il s'agit bien uniquement d'une erreur au niveau de son implémentation. De fait, certaines implémentations (en particulier NSS et OpenSSL) vérifient correctement la valeur de tous les octets de *padding* et ne sont pas concernées par cette vulnérabilité.

Recommandations

Le CERT-FR recommande de vérifier si les implémentations logicielles de TLS utilisées sont vulnérables à cette attaque et, le cas échéant, d'appliquer les correctifs de sécurité de l'éditeur dès que ceux-ci sont disponibles.

Documentation

– Article de la société FireEye :
https://www.fireeye.com/blog/threat-research/2014/12/is_poodle_back_fora.html
– Bulletin d'actualité CERTFR-2014-ACT-042 du 17 octobre 2014 :
http://www.cert.ssi.gouv.fr/site/CERTFR-2014-ACT-042
– Avis CERTFR-2014-AVI-533 du 18 décembre 2014 concernant F5 :
http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-533

3 - Avis de vigilance à l'approche des fêtes de fin d'année

A l'approche des fêtes de fin d'année, le CERT-FR souhaite rappeler que la période est particulièrement propice aux attaques informatiques. La baisse de vigilance durant cette période de congés favorise les tentatives de

compromission de systèmes d'information. En complément des recommandations habituelles du CERT-FR, nous attirons votre attention sur les points suivants :

- Les échanges de cartes de vœux électroniques représentent des vecteurs potentiels d'attaque car susceptibles de véhiculer des codes malveillants. Il importe que les utilisateurs soient sensibilisés à nouveau sur la possible réception de mails piégés pendant et après la période des fêtes.
- Il est recommandé de couper les accès internet non utilisés et d'appliquer un filtrage n'autorisant que les communications indispensables. Dans l'idéal, les accès pourront être restreints par l'emploi d'une liste blanche.
- La supervision des passerelles avec Internet et avec les serveurs critiques d'infrastructure doit être maintenue.

4 - Rappel des avis émis

Dans la période du 15 au 21 décembre 2014, le CERT-FR a émis les publications suivantes :

- CERTFR-2014-AVI-529 : Multiples vulnérabilités dans les produits F5
- CERTFR-2014-AVI-530 : Vulnérabilité dans les produits Huawei
- CERTFR-2014-AVI-531 : Vulnérabilité dans Struts
- CERTFR-2014-AVI-532 : Multiples vulnérabilités dans le noyau linux RedHat
- CERTFR-2014-AVI-533 : Vulnérabilité dans les produits F5
- CERTFR-2014-AVI-534 : Multiples vulnérabilités dans Huawei eSpace Desktop
- CERTFR-2014-AVI-535 : Vulnérabilité dans Apple Xcode
- CERTFR-2014-AVI-536 : Multiples vulnérabilités dans Huawei RomPager

Gestion détaillée du document

22 décembre 2014 version initiale.