Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 31 octobre 2013
N° CERTA-2013-ACT-044

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2013-ACT-044

1 - Compromission de site de « confiance » - PHP.NET

Le CERTA a récemment constaté l'insertion de données malveillantes au sein de la page d'accueil d'un site internet de « confiance » qui a ensuite été confirmée par l'éditeur.

En effet, le site officiel du langage PHP « php.net » a été victime d'une insertion de code subreptice, redirigeant à son insu le visiteur vers le domaine malveillant « url.whichusb.co.uk ».

Le CERTA recommande aux administrateurs de vérifier dans les journaux de connexions qu'aucune des stations de leur parc informatique ne s'est connectée à ce domaine. Dans le cas contraire, il est conseillé de lancer une analyse antivirus sur les machines impactées ou idéalement de réinstaller les stations de travail.

Cet incident nous rappelle que les sites de « confiance » doivent également faire l'objet d'une attention particulière. La mise à jour régulière des systèmes d'exploitation, antivirus et navigateurs, ainsi que l'installation de mécanismes de sécurité tel qu'*EMET* permettront de réduire le champs d'exposition aux failles applicatives des stations de travail.

Documentation

– Bulletin officiel :
http://www.php.net/archive/2013.php#id2013-10-24-2

2 - Nouvelles fonctionnalités de WordPress 3.7

WordPress a récemment publié la version 3.7 de son système de gestion de contenu (SGC) éponyme, qui apporte de nouvelles fonctionnalités de sécurité ainsi que divers correctifs. Parmi ces évolutions se distingue la capacité pour le SGC d'appliquer les correctifs de maintenance et de sécurité de manière automatique.

Dans le cadre des incidents qu'il est amené à traiter le CERTA constate régulièrement que les compromissions de sites Web gérés via des SGC se produisent majoritairement à cause d'une négligence dans l'application des correctifs, soit du coeur de l'application, soit des greffons qui l'accompagnent.

Le CERTA recommande donc aux utilisateurs de WordPress de migrer vers la branche 3.7 afin de bénéficier des fonctionnalités et des correctifs de sécurité qu'elle apporte. En complément de l'application des correctifs de sécurité doivent évidemment s'ajouter les traditionnelles mesures de défense en profondeur telles que le filtrage des flux, l'utilisation d'un pare-feu Web (WAF), la journalisation des évènements et la surveillance de ceux-ci ou encore le durcissement des moyens d'accès aux interfaces d'administration (utilisation de chiffrement asymétrique pour SSH, authentification à double facteur, filtrage par adresse IP source).

Documentation

– Guide de recommandation pour la sécurisation des sites Web :
http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-des-applications-web/recommandations-pour-la-securisation-des-sites-web.html

3 - Mise à jour Mozilla

Lors de la mise à jour du 29 octobre 2013 de Mozilla, 10 bulletins de sécurité ont été publiés.

Cinq de ces bulletins sont considérés comme critiques :

– MFSA 2013-93 impactant surtout Mozilla Firefox, cette mise à jour corrige quatre vulnérabilités (CVE-2013-5590, CVE-2013-5591, CVE-2013-5592 et CVE-2013-1792);
– MFSA 2013-98 impactant surtout Mozilla Firefox, cette mise à jour corrige une vulnérabilité (CVE-2013-5597);
– MFSA 2013-100 impactant surtout Mozilla Firefox, cette mise à jour corrige trois vulnérabilités (CVE-2013-5599, CVE-2013-5600 et CVE-2013-5601);
– MFSA 2013-101 impactant surtout Mozilla Firefox, cette mise à jour corrige une vulnérabilité (CVE-2013-5602);
– MFSA 2013-102 impactant surtout Mozilla Firefox, cette mise à jour corrige une vulnérabilité (CVE-2013-5603)

Toutes ces vulnérabilités peuvent mener un attaquant à exécuter du code arbitraire à distance.

Trois bulletins sont considérés comme importants (MFSA-2013-95, MFSA-2013-97 et MFSA-2013-99), certaines vulnérabilités permettent à un attaquant de provoquer une atteinte à la confidentialité des données.

Le CERTA recommande donc l'application de ces correctifs dès que possible.

Documentation

– Avis du CERTA-2013-AVI-613 :
http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-613/index.html

4 - Guide de l'ANSSI - Vulnérabilités 0-Day : prévention et bonnes pratiques

L'ANSSI a publié le 29 octobre 2013 un guide présentant une suite de bonnes pratiques permettant de limiter les risques liés aux vulnérabilités non corrigées dites 0-Day. Un 0-Day est une vulnérabilité non corrigée qui peut concerner tout type de logiciel (suite bureautique, application métier, système d'exploitation, logiciel embarqué, application mobile etc.) Ce type de vulnérabilité est susceptible d'être utilisé par des attaquants seul ou combiné à d'autres modes d'actions.

Pour mieux aider les DSI et les RSSI à répondre aux risques propres à ce type de vulnérabilité, l'ANSSI a publié le guide « Vulnérabilités 0-Day, prévention et bonnes pratiques ». Ce document répertorie les actions nécessaires en amont et en aval pour renforcer les systèmes d'information face à cette menace.

Ce guide vient en complément du guide d'hygiène de l'ANSSI et du bulletin CERTA-2012-ACT-038 qui proposait plusieurs mesures pouvant être mises en uvre sur les navigateurs Internet. Le CERTA recommande à ses lecteurs l'application de ces différentes mesures pour se prémunir au mieux des attaques 0-Day.

Documentation

– Guide de sécurité « Vulnérabilités 0-day : prévention et bonnes pratiques » :
http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-du-poste-de-travail-et-des-serveurs/vulnerabilites-0-day-prevention-et-bonnes-pratiques.html
– Bulletin d'actualité CERTA-2012-ACT-038 du 21 septembre 2012 « Navigateurs Internet : prévention des attaques 0day » :
http://www.certa.ssi.gouv.fr/site/CERTA-2012-ACT-038/

5 - Calendrier de formations du CFSSI

Le Centre de Formation à la Sécurité des Système d'Information (CFSSI) de l'ANSSI vient de publier le catalogue des formations qu'il dispensera au cour de l'année 2014.

Ce centre de formation, réservé aux personnels de l'administration française, propose une vingtaine de stages couvrant l'ensemble des domaines de la sécurité des systèmes d'information.

La liste ainsi que les fiches d'inscription aux stages sont disponibles en ligne, sur le site de l'ANSSI (cf. Documentation).

Documentation

- Catalogue des stages du CFSSI pour l'année 2014 :
  http://www.ssi.gouv.fr/fr/anssi/les-formations-du-cfssi/catalogue-des-stages.html

6 - Analyse et remédiation d'une vulnérabilité PHP

Le CERTA a pris connaissance de l'existence d'un code d'exploitation ciblant une vulnérabilité dans PHP. Cette vulnérabilité est connue (CVE-2012-1823) et a déjà été mentionnée dans l'avis CERTA-2013-AVI-358 concernant le logiciel Plesk.

Elle peut permettre à un attaquant d'exécuter du code PHP arbitraire sur un serveur vulnérable.

Description de la vulnérabilité

La vulnérabilité réside dans le fait que PHP, configuré en mode CGI, passe en ligne de commande certains paramètres contenus dans une requête HTTP si celle-ci commence par la chaîne « -d ». Un exemple d'une telle requête serait :

```
GET /index.php?-dsafe\_mode%3dOff+-dallow_url_include%3don
```

Ce comportement peut alors être exploité par une personne malveillante pour changer le paramétrage de certaines options de sécurité de PHP, notamment la possibilité de charger et d'exécuter un fichier PHP distant (directive « allow_url_include »).

Versions impactées

- PHP versions antérieures à 5.4.2
- PHP versions antérieures à 5.3.12

Élément de détection

Les tentatives d'exploitation peuvent être détectées en recherchant la chaîne « allow_url_include » dans les journaux d'un serveur web. Il faut cependant prendre soin de décoder au préalable les requêtes contenues dans les journaux, car un attaquant peut avoir procédé à un encodage au format « URL encoding » de ses requêtes pour tenter de contourner certains mécanismes de détection.

Remédiation

Le CERTA recommande de vérifier le niveau de mise à jour des installations de PHP et de migrer vers les versions stables les plus récentes pour bénéficier des dernières mises à jour de sécurité qui corrigent la vulnérabilité décrite dans cet article.

Documentation

Explication détaillée de la vulnérabilité :
http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823/

CVE-2012-1823 mitre :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1823

Format URL encoding :
http://en.wikipedia.org/wiki/Percent-encoding

Avis CERTA :
http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-358/CERTA-2013-AVI-358.html

7 - Rappel des avis émis

Dans la période du 25 au 30 octobre 2013, le CERTA a émis les publications suivantes :

- CERTA-2013-AVI-609 : Vulnérabilité dans EMC RSA
- CERTA-2013-AVI-610 : Multiples vulnérabilités dans McAfee Firewall Enterprise
- CERTA-2013-AVI-611 : Multiples vulnérabilités dans F5-ARX
- CERTA-2013-AVI-612 : Vulnérabilité dans EMC NetWorker

Gestion détaillée du document

31 octobre 2013 version initiale.