Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 10 mai 2013
N° CERTA-2013-ACT-019

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2013-ACT-019

1 Vulnérabilité critique dans Internet Explorer 8

Cette semaine, le CERTA a diffusé l'alerte CERTA-2013-ALE-003, concernant une vulnérabilité majeure dans *Internet Explorer 8*. Cette vulnérabilité est de type *Use-After-Free* (utilisation d'une donnée en mémoire après sa libération), dans la bibliothèque *mshtml.dll*. Son exploitation permet d'exécuter du code arbitraire à distance. Les recommandations émises dans le bulletin d'alerte sont :

- d'appliquer le correctif provisoire (fix) publié par *Microsoft* sur les navigateurs *Internet Explorer* à jour de leurs derniers correctifs afin de bloquer la majorité des attaques connues ;
- d'installer et de configurer l'outil de sécurité EMET sur les applications sensibles (dont *Microsoft Internet Explorer*) afin de limiter les risques connus d'exploitation ;
- d'utiliser *Microsoft Internet Explorer 9* ou supérieur qui ne sont pas concernés par cette vulnérabilité ;
- d'utiliser un navigateur alternatif maintenu et tenu à jour par son éditeur.

Dans le cadre d'une défense en profondeur contre les vulnérabilités dites 0day, plusieurs actions peuvent être menées en parallèle, afin de limiter l'impact des attaques les utilisant sur le système d'information, voire dans certains cas de les en empêcher. Ces mesures sont présentées dans le bulletin d'actualité CERTA-2012-ACT-038 (cf Documentation).

Documentation

- Alerte CERTA-2013-ALE-003 du 06 mai 2013 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-ALE-003/
- Bulletin de sécurité Microsoft 2847140 du 03 mai 2013 :
  http://technet.microsoft.com/en-us/security/advisory/2847140
- Correctif provisoire Microsoft 2847140 du 08 mai 2013 :
  http://support.microsoft.com/kb/2847140
- 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/
- Référence CVE CVE-2013-1347 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1347

2 Découverte de versions modifiées d'Apache comportant une porte dérobée

Lorsqu'un serveur Web est compromis, les attaquants peuvent injecter du contenu malveillant dans les pages Internet fournies par ce serveur. C'est une des raisons pour laquelle des utilisateurs qui visitent un site légitime, mais compromis, peuvent se retrouver infectés.

Les attaquants disposent de nombreuses méthodes pour injecter du contenu malveillant et cherchent généralement à les perfectionner afin de rester le plus discret possible. Cette tendance a récemment été constatée par la société Sucuri, spécialisée dans la sécurité Web. Cette société a découvert des serveurs compromis où le binaire du logiciel Apache a été remplacé par une version modifiée incorporant une porte dérobée. Selon des chercheurs d'ESET qui ont travaillé en collaboration avec Sucuri, cette porte dérobée est l'une des plus sophistiquées qu'ils ont observée jusqu'à présent.

Mis à part le binaire Apache modifié, aucune autre trace n'est présente sur le disque. Cette porte dérobée peut être contrôlée à distance grâce à des requêtes HTTP, non journalisées, et stocke sa configuration dans une zone de mémoire partagée, notamment entre tous les sous processus Apache. Son but est de rediriger les utilisateurs vers des kits d'exploitation, comme *Blackhole*, tout en essayant de ne pas rediriger les potentiels administrateurs, pour leur rendre plus difficile la détection et l'identification du problème.

Afin de déterminer si un serveur est infecté de cette manière, le CERTA recommande d'utiliser des utilitaires de vérification d'intégrité de fichiers. À titre d'exemple :

- lorsqu'un serveur Web, ou tout autre logiciel, a été installé à l'aide d'un gestionnaire de paquet, il est possible d'utiliser :
  - `debsums` pour les systèmes à base de paquets Debian,
  - `rpm` avec l'option `-verify` pour les systèmes à base de paquets RPM.
- il existe des solutions plus génériques comme le logiciel Samhain.

Il faut toutefois garder à l'esprit que les résultats de ces outils peuvent être faussés si les méta-données utilisées pour les vérifications ont également été modifiées par les attaquants.

Documentation

- Article relatant l'incident sur le blog de Sucuri :
  http://blog.sucuri.net/2013/04/apache-binary-backdoors-on-cpanel-based-servers.html
- Article de chercheurs d'ESET détaillant les fonctionnalités de la porte dérobée :
  http://www.welivesecurity.com/2013/04/26/linuxcdorked-new-apache-backdoor-in-the-wild-serves-blackhole/
- Logiciel Samhain, incluant des fonctionnalités de vérification d'intégrité :
  http://www.la-samhna.de/samhain/

3 Contrôle d'accès aux zones sensibles

Les zones sensibles d'un organisme telles que des salles serveur, des centraux téléphoniques ou encore un coeur de réseau nécessitent une attention particulière en termes de contrôle d'accès.

L'établissement et la mise à jour d'états recensant les personnels autorisés à accéder aux les zones les plus sécurisées devraient être systématiques.

De même, le départ d'un employé doit impliquer la révocation immédiate de ses droits d'accès et le changement des codes secrets partagés des systèmes de contrôle d'accès (mots de passe, digicode, armoires fortes, etc.) dont il avait connaissance.

À l'instar des incidents rencontrés récemment chez un opérateur français, l'actualité illustre régulièrement des cas où un ex-employé peut continuer à pénétrer dans des locaux protégés après son départ de l'entreprise, et y mener des actions malveillantes à l'encontre des infrastructures de son ancien employeur.

Documentation

- Article de presse du 26 avril 2013 :
  http://www.01net.com/editorial/594179/vandalisme-un-millier-de-foyers-coupes-dinternet-dans-les-yvelines/

4 Rappel des avis émis

Dans la période du 03 au 09 mai 2013, le CERTA a émis les publications suivantes :

- CERTA-2013-ALE-003 : Vulnérabilité dans Microsoft Internet Explorer 8
- CERTA-2013-AVI-285 : Vulnérabilité dans F5 Bind
- CERTA-2013-AVI-286 : Multiples vulnérabilités dans IBM Notes
- CERTA-2013-AVI-287 : Vulnérabilité dans Novell iPrint
- CERTA-2013-AVI-288 : Multiples vulnérabilités dans EMC Avamar
- CERTA-2013-AVI-289 : Vulnérabilité dans EMC NetWorker
- CERTA-2013-AVI-290 : Multiples vulnérabilités dans Xen
- CERTA-2013-AVI-291 : Vulnérabilité dans Novell ZENworks
- CERTA-2013-AVI-292 : Vulnérabilité dans des équipements Huawei
- CERTA-2013-AVI-293 : Multiples vulnérabilités dans EMC Archer GRC
- CERTA-2013-AVI-294 : Vulnérabilité dans nginx

Gestion détaillée du document

10 mai 2013 version initiale.