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 28 mars 2014
N° CERTFR-2014-ACT-013

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2014-ACT-013

1 - Attaques exploitant la fonctionnalité pingback du CMS WordPress

Récemment la presse s'est fait l'écho d'attaques en déni de service distribué visant les sites utilisant le système de gestion de contenu *WordPress*. Cette attaque est rendue possible via la fonctionnalité « pingback » initialement prévue pour permettre le référencement croisé des blogs. Le mécanisme incriminé fonctionne de la façon suivante :

- un blogueur écrit un article sur son site ;
- un second blogueur mentionne l'article sur son propre site ;
- si la fonctionnalité est activée, un commentaire est automatiquement effectué sur le site original via une requête XML-RPC, appelée « ping ».

Le service XML-RPC étant activé par défaut et ne requérant pas d'authentification, l'envoi massif de requêtes falsifiées provenant soi-disant d'un site A vers un site B, conduit le site B à effectuer en retour des requêtes vers le site A. Employé à grande échelle, ce mécanisme consomme de la bande passante et de la ressource sur les serveurs Web des deux sites, visant à saturer le service du site cible.

Il est relativement aisé de détecter si un site sous *WordPress* a été impliqué dans une telle attaque à l'insu de son propriétaire, notamment en vérifiant dans les journaux Web la présence d'un nombre excessif de requêtes `HTTP POST` à destination de pages nommées « xmlrpc.php ».

Il est possible de désactiver la fonctionnalité de « pingback » dans les options de chaque article publié sur le site. La désactivation complète du service XML-RPC, bien que plus délicate, est envisageable si aucun autre greffon ou aucune autre fonctionnalité du CMS ne l'exploitent.

Documentation

- *WordPress* et la fonctionnalité pingback :
  http://en.support.WordPress.com/comments/pingbacks/

2 - Vulnérabilité dans Microsoft Word

Le 25 mars, Microsoft a publié sur son blog technique un article concernant une vulnérabilité non corrigée dans le logiciel de traitement de texte Word. Cette vulnérabilité CVE-2014-1761 touche toutes les versions de Word actuellement supportées par l'éditeur. Microsoft a pu observer des attaques ciblées exploitant cette vulnérabilité sous Word 2010.

Protections disponibles dans Microsoft Office

Comme détaillé dans le bulletin d'alerte du CERT-FR, une exploitation réussie de cette vulnérabilité, via l'envoi d'un fichier RTF malveillant, permet à un attaquant d'exécuter du code arbitraire. Microsoft a publié un correctif provisoire permettant de bloquer l'ouverture d'un fichier RTF avec Word. Ce correctif est appliqué via la modification des réglages de configuration du centre de gestion de la confidentialité (« Trust Center »). Ce centre regroupe

les différents paramètres de sécurité et de confidentialité de Word et plus globalement de la suite Microsoft Office. Une liste non exhaustive de mesures permettant de renforcer la sécurité du logiciel est présentée ci-dessous :

- bloquer un ou plusieurs formats de fichiers ;
- forcer la vérification de signatures numériques ;
- forcer l'ouverture d'un type de fichier en mode protégé.

Parmi les mesures décrites précédemment, le mode protégé disponible depuis la suite Microsoft Office 2010 limite les risques lors de l'ouverture d'un fichier malveillant et en particulier bloque la vulnérabilité CVE-2014-1761. En effet, ce mode ouvre le fichier en lecture seule et n'autorise pas les contrôles ActiveX à se charger.

Recommandations

Comme expliqué dans la section « Contournement provisoire » du bulletin d'alerte du CERT-FR, l'application de la mesure provisoire « Fix it 51010 » publiée par Microsoft empêche l'ouverture de fichiers RTF depuis Word. Il est également possible pour une organisation de s'appuyer sur la définition d'une stratégie de groupe (GPO) Active Directory pour déployer sur l'ensemble d'un parc :

- soit une mesure permettant de bloquer l'ouverture des fichiers RTF depuis Word ;
- soit une mesure permettant de forcer l'ouverture des fichiers RTF en mode protégé pour les versions de Microsoft Word qui supportent cette fonctionnalité (Word 2010 et 2013).

Enfin, l'installation et la configuration de l'outil de sécurité EMET permet de limiter les risques connus d'exploitation.

Documentation

- Bulletin d'alerte du CERT-FR CERTFR-2014-ALE-002 :
  http://www.cert.ssi.gouv.fr/site/CERTFR-2014-ALE-002/index.html
- Détails du mode protégé de la suite Microsoft Office :
  http://office.microsoft.com/fr-fr/word-help/quest-ce-que-le-mode-protege-HA010355931.aspx
- Security Advisory 2953095 Microsoft :
  http://blogs.technet.com/b/srd/archive/2014/03/24/security-advisory-2953095-recommendation-to-stay-protected-and-for-detections.aspx

3 - Risques liés à l'autoconfiguration d'IPv6

Par défaut, les systèmes d'exploitation récents supportent tous le protocole IPv6 en plus d'IPv4. Le principal intérêt d'IPv6 est la taille de l'espace d'adressage, bien plus importante qu'avec IPv4 (128 bits contre 32 bits). Comme il n'existe pas de compatibilité entre les adresses IPv4 et IPv6, les systèmes d'exploitation implémentent les deux piles, qui sont activées par défaut. Cela signifie que les machines d'un réseau qui repose sur un adressage IPv4 peuvent également communiquer via IPv6, notamment grâce à la fonctionnalité d'autoconfiguration.

Une adresse IPv6 est composée de 3 blocs :

- préfixe (48 bits) : topologie publique ;
- sous-réseau (16 bits) : topologie privée ;
- interface (64 bits) : spécifique à l'interface réseau de l'hôte (dérivée de l'adresse MAC).

Pour des questions de protection de la vie privée (possibilité de traquer une machine), la partie interface peut reposer sur des données aléatoires renouvelées fréquemment. Le préfixe définit le domaine de validité et d'unicité. Par défaut, une interface réseau disposera d'une adresse de type "lien local" (préfixe `fe80::/10`), qui n'est pas routable. Cette dernière est notamment utilisée par le protocole de découverte des voisins (NDP) qui permet entre autres l'autoconfiguration. Il est possible de voir si une interface réseau dispose d'une adresse IPv6 attribuée par le mécanisme d'autoconfiguration (commençant par `fe80`) en utilisant la commande "`ipconfig /all`" sous Windows ou son équivalent "`ifconfig -a`" sous Linux.

La fonctionnalité de configuration automatique permet d'obtenir des paramètres comme le préfixe du réseau, le MTU, mais également l'adresse des serveurs DNS récursifs (RDNSS) grâce aux messages d'annonce de routeur et peut fonctionner selon plusieurs modes :

- le mode sans état : seul le préfixe est fourni et l'hôte construit lui-même l'adresse IPv6 pour l'interface réseau ;
- le mode avec état : une adresse complète est fournie à l'hôte, soit directement dans le message d'annonce de routeur, soit par l'intermédiaire du protocole DHCPv6.

Il est de plus possible de combiner les deux modes pour obtenir par exemple le préfixe du réseau dans le message d'annonce de routeur et la configuration DNS par l'intermédiaire du protocole DHCPv6 (en positionnant le drapeau « Other Configuration » dans le message d'annonce de routeur). Selon les systèmes d'exploitation, il est également possible de se passer des messages d'annonce de routeur et d'envoyer directement une requête au serveur DHCPv6.

Lorsqu'une machine dispose à la fois d'une configuration (adresse IP, serveur DNS, etc.) IPv4 et IPv6, de nombreux applicatifs vont par défaut privilégier l'utilisation d'IPv6 (par exemple Internet Explorer ou Mozilla Firefox). Si un attaquant parvient à introduire un service d'annonce de routeur IPv6 et/ou un serveur DHCPv6 dans un réseau IPv4 sur lequel des machines disposent d'interfaces réseau IPv6 supportant l'autoconfiguration, il est possible de réaliser une attaque de type « homme du milieu » en indiquant par exemple un serveur DNS non légitime. L'attaquant utilisera ensuite les mécanismes NAT64 et DNS64 de façon à relayer les requêtes de la victime sur le reste du réseau IPv4.

Pour se prémunir contre ce type d'attaque, le CERT-FR recommande :

- de désactiver, si cela n'entraîne pas d'incompatibilité, le support de l'IPv6 dans le système d'exploitation;
- si IPv6 est activé, de maîtriser et surveiller le trafic concernant notamment les messages d'annonce de routeur et le protocole DHCPv6. Des mécanismes de sécurité implémentés sur certains commutateurs permettent de s'en prémunir (*RA Guard*, *DHCPv6 Guard*). Sur les systèmes Linux, le pare-feu *ip6tables* devra également être mis en place et correctement configuré.

Dans tous les cas et pour appliquer le principe de défense en profondeur, l'utilisation de protocoles applicatifs sécurisés (HTTPS par exemple) est recommandée pour rendre inefficace l'exploitation d'attaques de type « homme du milieu ».

4 - Rappel des avis émis

Dans la période du 21 au 27 mars 2014, le CERT-FR a émis les publications suivantes :

- CERTFR-2014-ALE-002 : Vulnérabilité dans Microsoft Word
- CERTFR-2014-AVI-139 : Vulnérabilité dans OpenSSH
- CERTFR-2014-AVI-140 : Vulnérabilité dans IBM Rational ClearCase
- CERTFR-2014-AVI-141 : Multiples vulnérabilités dans IBM Cognos Express
- CERTFR-2014-AVI-142 : Multiples vulnérabilités dans IBM InfoSphere BigInsights
- CERTFR-2014-AVI-143 : Vulnérabilité dans IBM OS/400
- CERTFR-2014-AVI-144 : Vulnérabilité dans le noyau Linux
- CERTFR-2014-AVI-145 : Vulnérabilité dans le noyau Linux
- CERTFR-2014-AVI-146 : Vulnérabilité dans le noyau Linux
- CERTFR-2014-AVI-147 : Vulnérabilité dans Mozilla Firefox pour Android
- CERTFR-2014-AVI-148 : Multiples vulnérabilités dans IBM Lotus Protector for Mail Security
- CERTFR-2014-AVI-149 : Vulnérabilité dans Cisco IOS
- CERTFR-2014-AVI-150 : Multiples vulnérabilités dans Cisco IOS
- CERTFR-2014-AVI-151 : Vulnérabilité dans Cisco IOS
- CERTFR-2014-AVI-152 : Vulnérabilité dans Cisco IOS
- CERTFR-2014-AVI-153 : Vulnérabilité dans Cisco IOS

Gestion détaillée du document

28 mars 2014 version initiale.