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 01 décembre 2014
N° CERTFR-2014-ACT-048

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2014-ACT-048

1 - Mise à jour de sécurité Adobe Flash Player

Le 14 octobre 2014, Adobe a publié une mise à jour de sécurité (bulletin de sécurité APSB14-22) concernant les vulnérabilités suivantes, pouvant conduire à une exécution de code arbitraire :

- CVE-2014-0564 et CVE-2014-0558 (critiques) concernant deux corruptions de mémoire ;
- CVE-2014-0569 (critique) concernant un dépassement d'entier.

Un bulletin complémentaire (APSB14-26) a été publié le 25 novembre 2014, en dehors du cycle habituel de mise à jour de l'éditeur. Il porte sur la vulnérabilité CVE-2014-8439 (critique), qui concerne un déréférencement de pointeur pouvant potentiellement conduire à une exécution de code arbitraire.

Adobe recommande l'application de ce correctif. Microsoft et Google ont également publié des mises à jour de leurs navigateurs respectifs Internet Explorer (10 et 11) et Chrome pour corriger les versions embarquées de Flash Player.

Le CERT-FR rappelle l'importance de ces correctifs de sécurité et recommande ainsi leur application dès que possible.

Documentation

- http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-497/index.html
- http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-496/index.html
- http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-431/index.html
- https://helpx.adobe.com/security/products/flash-player/apsb14-22.html
- https://helpx.adobe.com/security/products/flash-player/apsb14-26.html
- http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8439
- https://technet.microsoft.com/library/security/2755801
- http://googlechromereleases.blogspot.fr/2014/11/stable-channel-update$_2$5.$html$

2 - Vague de rançongiciels

Le CERT-FR a été informé d'une campagne récente de messages électroniques malveillants qui installent un rançongiciel sur les systèmes victimes.

Un rançongiciel (ou ransomware) est un programme qui rend immédiatement inaccessible des fichiers de la victime, en général les documents bureautiques présents dans le répertoire « Mes documents » ainsi que dans tous les disques réseau ouverts en écriture à l'utilisateur. Ces documents sont chiffrés par le rançongiciel : les fichiers originaux sont eux supprimés. Un message de chantage est ensuite placé sur le bureau de l'utilisateur, exigeant le paiement d'une somme d'argent en échange du déchiffrement de ses documents.

Les messages d'hameçonnage utilisent des techniques d'ingénierie sociale classiques indiquant par exemple que « *Vous avez un paiement en attente* », pour inciter la victime à suivre un lien hypertexte et provoquer le téléchargement et l'exécution du maliciel.

Les techniques observées dans cette campagne sont multiples : téléchargement direct d'un exécutable, téléchargement d'une archive contenant un exécutable, ou redirection sur un contenu flash qui exploite une vulnérabilité du lecteur.

Le CERT-FR vous recommande les actions de prévention suivantes :

- la sensibilisation des utilisateurs : de nombreux messages de cette campagne sont non sollicités, d'un émetteur inconnu et contiennent de nombreuses fautes orthographiques ;
- l'utilisation des « *Software Restriction Policies* » pour interdire l'exécution de logiciels dans les répertoires temporaires ;
- la sauvegarde régulière des fichiers des utilisateurs ;
- la mise à jour des bases de signatures anti-virus ;
- la protection des partages de fichiers, par exemple en positionnant les permissions des dossiers partagés en lecture seule ;
- l'application des correctifs de sécurité, en priorité les postes exposés sur Internet (système et applications).

Si l'un de vos utilisateurs est victime de ce type de maliciel, le CERT-FR conseille la conduite suivante :

- isoler au plus vite le poste du réseau ;
- identifier le message malveillant et rechercher d'éventuels autres destinataires afin de les prévenir du risque encouru ;
- bloquer sur le serveur mandataire l'accès aux domaines ou URLs identifiés dans le message malveillant ;
- reformater le poste client et réinstaller un système sain ;
- restaurer les copies de sauvegarde des fichiers modifiés.

Le versement de la rançon par l'attaquant ne garantit en rien le déchiffrement des fichiers et le stockage sécurisé des informations de paiement. Il peut au contraire provoquer l'installation de maliciels supplémentaires sur le poste compromis.

- Recommandation pour la mise en œuvre d'une politique de restrictions logicielles sous Windows : http://www.ssi.gouv.fr/IMG/pdf/NP_Applocker_NoteTech-v1.pdf
- Site stop ransomware : http://stopransomware.fr

3 - Synchronisation automatisée de données hébergées par des services en nuage

La plupart des applications ou des systèmes d'exploitation récents offrent de plus en plus souvent des solutions de sauvegarde de données dans le nuage. Les données ainsi téléversées sont variées. Elles sont composées principalement de paramètres de personnalisation, d'événements du calendrier, de contacts, de notes, de documents ainsi que des données plus sensibles telles que mots de passe ou numéros de carte bancaire.

La synchronisation de ces données remplit plusieurs objectifs. Le plus courant est de garantir l'accès aux informations, que ce soit pour une édition coopérative de documents, un partage de photos entre proches ou un accès depuis plusieurs dispositifs (ordiphone, navigateur internet...).

Activation des services de synchronisation

Dans la plupart des cas, il est possible d'activer ou de désactiver la mise en nuage automatique des données. Ces paramètres sont généralement activés par défaut. Il est donc recommandé que l'utilisateur en prenne connaissance et vérifie régulièrement la configuration de ses systèmes et applications. Cependant, certains services ne permettent pas de désactiver les fonctions de sauvegarde automatique en ligne car il s'agit du service principal qu'ils proposent. C'est le cas par exemple des éditeurs de documents hébergés en nuage.

Recommandations

Il est recommandé de ne pas conserver en nuage des données sensibles et de s'assurer (via les procédures décrites dans les pages liées ci-dessous) que la synchronisation automatique en nuage de ces informations est

désactivée. De plus, le CERT-FR recommande de vérifier régulièrement les paramètres de synchronisation en nuage, surtout après les mises à jour de logiciels ou de systèmes d'exploitation. En effet, de nouveaux paramètres liés à l'envoi automatique de données sur internet peuvent apparaître ou encore voir leur valeur par défaut changer.

Enfin, il est important de comprendre que les services d'hébergement en nuage ne garantissent pas forcément la confidentialité des données hébergées. Dans le cas de données sensibles, il est recommandé de les protéger contre la lecture par un tiers à l'aide des méthodes de chiffrement appropriées.

Procédures de désactivation de la synchronisation automatique

- Applications mobiles Google (Android et iOS)
  https://support.google.com/plus/answer/1304820?hl=fr
- iCloud
  http://support.apple.com/kb/PH2613?viewlocale=fr_FR
- Windows 8
  http://windows.microsoft.com/fr-fr/windows-8/sync-settings-pcs

4 - Rappel des avis émis

Dans la période du 24 au 30 novembre 2014, le CERT-FR a émis les publications suivantes :

- CERTFR-2014-AVI-493 : Multiples vulnérabilités dans Asterisk
- CERTFR-2014-AVI-494 : Multiples vulnérabilités dans phpMyAdmin
- CERTFR-2014-AVI-495 : Multiples vulnérabilités dans le noyau linux Ubuntu
- CERTFR-2014-AVI-496 : Vulnérabilité dans Adobe Flash Player
- CERTFR-2014-AVI-497 : Vulnérabilité dans Google Chrome
- CERTFR-2014-AVI-498 : Multiples vulnérabilités dans Docker
- CERTFR-2014-AVI-499 : Multiples vulnérabilités dans les produits F5
- CERTFR-2014-AVI-500 : Multiples vulnérabilités dans les systèmes SCADA Siemens
- CERTFR-2014-AVI-501 : Multiples vulnérabilités dans Wordpress
- CERTFR-2014-AVI-502 : Multiples vulnérabilités dans les produits F5

Gestion détaillée du document

01 décembre 2014 version initiale.