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 09 février 2015
N° CERTFR-2015-ACT-006

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2015-ACT-006

1 - Rappel des vulnérabilités récentes dans Adobe Flash Player

Adobe Flash Player est utilisé principalement par les navigateurs Internet pour afficher du contenu dynamique sur des pages web.

Depuis le début de l'année, plusieurs vulnérabilités sur Adobe Flash Player ont été signalées par le CERT-FR, à travers des avis 2015-019, 2015-037, 2015-039 et l'alerte CERTFR-2015-ALE-001.

Plusieurs organismes rapportent que ces vulnérabilités sont activement exploitées par des attaquants. Des exploits sont par ailleurs disponibles dans des kits d'exploitation.

Vulnérabilités Flash CVE-2015-0313

Le 02 février 2015, le CERT-FR a publié l'alerte CERTFR-2015-ALE-002, portant sur une vulnérabilité non corrigée au sein d'Adobe Flash Player.

Détails techniques

D'après la société Trustwave, le problème réside dans l'exploitation d'une vulnérabilité de type `use-after-free` située dans une fonctionnalité de Flash nommée `FlashCC` qui concerne l'accès à la mémoire. Cette fonctionnalité permet d'accélérer l'accès à la mémoire du processus en utilisant un code ActionScript.

Pour exploiter cette vulnérabilité, une partie de cette mémoire est mappée dans un objet Flash de type `ByteArray`, qui est pointé par le champ `domainMemory` d'un objet de type `ApplicationDomain`.

Lorsque l'objet `ByteArray` est libéré, le champ `domainMemory` pointe toujours sur la mémoire du processus. Une pulvérisation du tas va ensuite permettre de remplir cet espace avec des objets de type `Vector`. L'utilisation du champ `domainMemory` change la taille d'un de ces objets `Vector`. Ce dernier permet d'avoir accès en lecture et en écriture à l'ensemble de la mémoire du processus.

Cette vulnérabilité permet d'exécuter du code arbitraire à distance avec les privilèges du processus exploité. Elle ne semble pas pouvoir outrepasser les protections de type bac à sable des navigateurs.

Un exploit se serait propagé grâce à des régies publicitaires compromises affichant des publicités sur des sites très fréquentés tels que *dailymotion.com*, *huffingtonpost.com* ou *answers.com*.

Versions affectées

Cette vulnérabilité affecte les versions 16.0.0.296 et antérieures sur Windows et Macintosh ainsi que les versions 13.x antérieures à la 13.0.0.264 sur Linux. Les cas d'exploitation observés sont restreints au système d'exploitation Windows, toutes versions confondues (incluant 8.1).

Distribution du correctif

Adobe a indiqué le 04 février qu'un correctif allait être déployé automatiquement aux utilisateurs ayant activé les mises à jour automatiques. Cette nouvelle version, estampillée 16.0.0.305, est disponible dès maintenant sur la page
https://get.adobe.com/fr/flashplayer/ .

En conséquence, l'alerte CERTFR-2015-ALE-002 a été fermée le 05 février 2015.

Recommandations

Le CERT-FR recommande de désactiver l'exécution automatique de code Flash au sein des navigateurs jusqu'à installation du correctif.

Le CERT-FR conseille également d'installer des outils permettant de durcir les systèmes et de rendre l'exploitation de vulnérabilités plus difficile. En particulier, sous Windows, l'outil EMET proposé par Microsoft, permet de limiter les risques d'exploitation (voir Documentation).

Enfin le CERT-FR préconise d'activer les mises à jour automatiques pour l'ensemble des logiciels.

Documentation

- Rapports de sécurité Adobe:
  - https://helpx.adobe.com/security/products/flash-player/apsa15-01.html
  - https://helpx.adobe.com/security/products/flash-player/apsb15-02.html
  - https://helpx.adobe.com/security/products/flash-player/apsa15-02.html
- Avis et alerte du CERT-FR:
  - http://www.cert.ssi.gouv.fr/site/CERTFR-2015-ALE-001/index.html
  - http://www.cert.ssi.gouv.fr/site/CERTFR-2015-AVI-019/index.html
  - http://www.cert.ssi.gouv.fr/site/CERTFR-2015-AVI-037/index.html
  - http://www.cert.ssi.gouv.fr/site/CERTFR-2015-AVI-039/index.html
- EMET 5.1:
  - http://www.microsoft.com/emet
- Rapport Trustwave:
  - https://www.trustwave.com/Resources/SpiderLabs-Blog/A-New-Zero-Day-of-Adobe-Flash-CVE-2015-0313-Exploited-in-the-Wild/

2 - Rappel des moyens de contact du CERT-FR

Au sein du Centre Opérationnel de la Sécurité des Systèmes d'Information (COSSI) de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), le CERT-FR apporte son soutien en matière de gestion d'incidents aux ministères, institutions, juridictions, autorités administratives indépendantes, collectivités territoriales et OIV (Opérateurs d'Importance Vitale).

Il est le point de contact international privilégié pour tout incident de nature cyber touchant la France. Il assure une permanence de ses activités 24h/24, 7j/7.

Le CERT-FR peut être contacté :

- Par téléphone :
  - +33 (0)1 71 75 84 50 pendant les heures ouvrables (du lundi au vendredi de 8h30 à 18h30) ;
  - ou +33 (0)1 71 75 84 68 en dehors des heures ouvrables ;
- Par télécopie : +33 (0)1 84 82 40 70
- Par courriel : contact@cert.ssi.gouv.fr

Pour échanger des informations chiffrées, deux moyens de chiffrement peuvent être utilisés :

- Clé PGP
  - Identifiant de la clé : 0x1B45CF2A
  - Empreinte de la clé : 7F4C 8FA6 A356 D1CC 2E5C AB09 5416 33B8 1B45 CF2A

  - Télécharger la clé publique :
    http://www.cert.ssi.gouv.fr/cert-fr/public_key.asc
- Clé ACID : Pour un échange de clés publiques ACID, veuillez contacter le CERT-FR pendant les heures ouvrables.

Veuillez enfin noter que :
- Le CERT-FR n'est pas un service de justice ou de police recevant des plaintes.
- Le CERT-FR a choisi de ne pas être présent sur les réseaux sociaux et n'y a ouvert aucun compte.

Liens utiles

- Comment contacter le CERT-FR :
  http://www.cert.ssi.gouv.fr/cert-fr/contact.html
- Comment contacter le COSSI :
  http://www.ssi.gouv.fr/IMG/pdf/Fiche_contacts_COSSI_internet.pdf

3 - SSDP et déni de service

Le protocole Simple Service Discovery Protocol (SSDP) est utilisé, entres autres, pour détecter des équipements UPnP (« *Universal Plug Play* ») à travers le réseau. Ce protocole est utilisé par un certain nombre d'équipements (comme des routeurs domestiques, par exemple), mais aussi par des périphériques du type télévision, NAS etc.

Une mauvaise configuration d'un service implémentant le protocole SSDP permet à des attaquants de réaliser des attaques de type déni de service distribué par amplification.

Le principe de ce type d'attaque est d'usurper l'adresse IP d'une cible et d'envoyer des requêtes à un service tiers afin de générer une réponse de taille supérieure à la requête initiale.

SSDP reposant sur UDP, protocole non connecté, il n'est pas possible de se prémunir contre l'usurpation d'adresse IP source. L'attaquant envoie donc des datagrammes UDP forgés, ayant pour IP source l'adresse de la victime, à des équipements mal configurés et qui utilisent SSDP. La réponse est alors envoyée à la victime.

Le CERT-FR recommande de désactiver les services UPnP sur les équipements lorsque le service n'est pas nécessaire. Par ailleurs, la configuration des équipements pour lesquels UPnP est nécessaire doit être modifiée afin que ceux-ci n'écoutent plus sur les interfaces externes et ne répondent plus aux requêtes externes à l'entité. Enfin, il est recommandé de filtrer le trafic SSDP (port UDP 1900) à la bordure de l'entité hébergeant les équipements potentiellement exploitables.

Documentation

- Dénis de service, prévention et réaction :
  http://www.cert.ssi.gouv.fr/site/CERTA-2012-INF-001/

4 - Rappel des avis émis

Dans la période du 02 au 08 février 2015, le CERT-FR a émis les publications suivantes :

- CERTFR-2015-ALE-002 : Vulnérabilité dans Adobe Flash Player
- CERTFR-2015-ALE-003 : Nouvelle campagne d'hameçonnage de type rançongiciel
- CERTFR-2015-AVI-049 : Vulnérabilité dans EMC Avamar
- CERTFR-2015-AVI-050 : Multiples vulnérabilités dans les produits IBM
- CERTFR-2015-AVI-051 : Multiples vulnérabilités dans le noyau Linux de Red Hat
- CERTFR-2015-AVI-052 : Multiples vulnérabilités dans IBM Tivoli Storage Manager
- CERTFR-2015-AVI-053 : Multiples vulnérabilités dans VLC Media Player
- CERTFR-2015-AVI-054 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu
- CERTFR-2015-AVI-055 : Vulnérabilité dans Adobe Flash Player
- CERTFR-2015-AVI-056 : Vulnérabilité dans Cisco WebEx Meetings Server
- CERTFR-2015-AVI-057 : Multiples vulnérabilités dans les produits IBM
- CERTFR-2015-AVI-058 : Multiples vulnérabilités dans Google Chrome

Gestion détaillée du document

09 février 2015 version initiale.

Conditions d'utilisation de ce document :	http://cert.ssi.gouv.fr/cert-fr/apropos.html
Dernière version de ce document :	http://cert.ssi.gouv.fr/site/CERTFR-2015-ACT-006