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 24 janvier 2014
N° CERTFR-2014-ACT-004

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2014-ACT-004

1 - Création du CERT-FR

Le 21 janvier 2014, le CERTA a changé de nom pour devenir le CERT-FR (Computer Emergency Response Team - France).

Le CERT-FR est le CERT gouvernemental français. Il apporte son soutien en matière de gestion d'incidents aux ministères, institutions, juridictions, autorités 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.

Les activités du CERT-FR peuvent être réparties selon deux catégories. La première, pour mieux percevoir la menace, couvre :

- une veille active sur les vulnérabilités menaçant les systèmes d'information, l'étude de leur exploitabilité et leur mode de détection, la proposition de contre-mesures pertinentes et l'élaboration d'avis et d'alertes ;
- des échanges techniques avec les éditeurs des produits et les autres CSIRT ;
- des audits et des inspections de sécurité (tests d'intrusion, audits de configuration, audit de code, etc.) ;
- le développement et l'exploitation de sondes de détection au profit des ministères, ainsi que le partage de signatures.

La seconde, en réaction et en réponse à un incident de sécurité couvre :

- la collecte d'éléments techniques, l'analyse et la qualification de la cause, une meilleure compréhension des scénarios d'attaque et de l'étendue de la compromission ;
- la définition de mesures d'assainissement et de durcissement ;
- la coordination avec les partenaires et les victimes dans les gestions de crise ou d'incidents ;
- des synthèses et une capitalisation des informations issues des incidents traités ;
- la conduite de campagnes de recherche de victimes.

Dans le cadre de ce changement de dénomination, veuillez noter les coordonnées du CERT-FR :

- Mél : contact@cert.ssi.gouv.fr
- Web : www.cert.ssi.gouv.fr
- Tél heures ouvrées : 01 71 75 84 50 (de 08h30 à 18h30)
- Tél heures non ouvrées : 01 71 75 84 68

Documentation

- Du CERTA au CERT-FR :
  http://www.cert.ssi.gouv.fr/cert-fr/certfr.html
- Nous contacter :
  http://www.cert.ssi.gouv.fr/cert-fr/contact.html
- La clé PGP du CERT-FR :
  http://www.cert.ssi.gouv.fr/cert-fr/public_key.asc

2 - Risques liés au format PDF et recommandations

Le format PDF et les risques liés à son utilisation

Le format de fichier PDF (Portable Document Format), créé par la société Adobe System en 1990, permet la création de documents dont la mise en forme est préservée (polices, images, etc.) telle qu'elle a été définie lors de leur création, et ce y compris lorsque le fichier est ouvert avec un logiciel d'édition ou un système d'exploitation différent de ceux de l'auteur.

PDF est un format dit « ouvert », c'est-à-dire que la société Adobe en a diffusé les spécifications, tout en restant néanmoins propriétaire des droits. Ce modèle a permis de faire apparaître de nombreux logiciels tiers compatibles avec ce type de fichiers (Foxit, Sumatra PDF, Evince, Xpdf, Okular, etc.). Par ailleurs, il est à noter que l'utilisation d'ActiveX permet la lecture PDF dans les navigateurs Internet Explorer sans aucune action nécessaire de la part de l'utilisateur.

Son important taux de pénétration dans les systèmes d'information et plus généralement dans notre quotidien (99% des postes utilisateurs possèdent au moins un lecteur PDF) et son taux d'utilisation significatif comparativement aux autres formats d'édition de texte (on peut estimer que de l'ordre de 70% des documents textes formatés échangés sur l'Internet le sont dans ce format) en font un format privilégié par les attaquants pour compromettre des postes utilisateurs (exécution de code arbitraire). Ceci s'explique par ailleurs par les nombreuses fonctionnalités offertes par le format, ouvrant une surface d'attaque importante. Adobe Reader est en particulier capable de :

- gérer des formulaires (AcroForm),
- réaliser des actions automatisées (OpenAction),
- exécuter des scripts au format JavaScript (JS),
- embarquer de nombreux formats de fichiers (dont Flash, Word, Excel, MP3, TIFF, etc.),
- afficher et interpréter des hyperliens,
- afficher des annotations,
- supporter le chiffrement de document à l'aide d'un mot de passe,
- etc.

Les objets (pages, actions, scripts, images, références, etc.) contenus dans un document PDF sont normalement référencés dans une table globale, appelée xref. L'une des opportunités dont dispose l'attaquant réside dans le fait qu'il peut exister des objets non référencés dans cette table, qui ne seront donc pas nativement pris en compte par les logiciels d'édition pour l'affichage d'informations de contenu du document, mais qui au contraire peuvent être exploités par l'attaquant pour cacher des informations (charges malveillantes, données à exfiltrer, leurres, etc.).

De plus, les spécifications actuelles de PDF autorisent l'utilisation de nombreux algorithmes de compression (JBIG2, LZW, FLATE, RLE, CCITT, etc.) et d'encodage des objets compris dans le document. Ceci permet d'avoir des documents de plus petite taille, mais offre aussi de nouvelles possibilités pour une personne malintentionnée de compliquer l'analyse à des fins de sécurité de tels documents (d'où certaines limitations des antivirus, que ce soit au niveau réseau ou sur les postes utilisateurs).

A titre d'illustration, ont été recensées sur les trois dernières années 153 vulnérabilités touchant Adobe Reader, le logiciel de référence en matière de lecture de PDF (cve.mitre.org).

Exemples de vulnérabilités

La CVE-2013-0640 est une vulnérabilité qui touche Adobe Reader, dans ses versions 9.X (<9.5.4), 10.X (<10.1.6) et 11.X (<11.0.02), et qui permet à un attaquant d'exécuter du code à distance lors de l'ouverture du document piégé. Cette faille est encore largement utilisée lors d'attaques ciblées (http://www.alienvault.com/open-threat-exchange/blog/new-sykipot-developments). La vulnérabilité se situe au niveau de la gestion de la mémoire des objets des formulaires AcroForm XFA ou AcroForm FDF.

Un document malveillant exploitant cette vulnérabilité contient, outre ses éventuels objets légitimes :

- un objet de type AcroFrom XFA ou AcroFrom FDF représentant le formulaire,
- un objet de type JS (JavaScript) qui manipule les éléments du formulaire et réalise une attaque par pulvérisation des segments de mémoire (heap spray),
- un objet optionnel de type OpenAction qui lance automatiquement le script à l'ouverture du PDF.

La CVE-2012-0754 est une vulnérabilité qui touche Adobe Reader, dans ses versions 10.X (<10.3.183.15), 11.X (<11.1.102.62) et 11.X (<11.1.111.6) sur les plateformes Android, et qui permet à un attaquant d'exécuter du code à distance lors de l'ouverture du document piégé. Cette faille a été largement utilisée lors d'attaque ciblées

(http://contagiodump.blogspot.fr/2012/03/mar-2-cve-2012-0754-irans-oil-and.html). La vulnérabilité se situe au niveau de la gestion de la mémoire lors de l'analyse syntaxique des vidéos au format MP4 dans le module Flash intégré à Adobe Reader.

Un document malveillant exploitant cette vulnérabilité contient, outre ses éventuels objets légitimes :

- un objet de type Flash contenant le chargeur de fichier MP4,
- un objet de type EF (Embedded File) représentant le fichier vidéo MP4.

Durcissement de la configuration d'Adobe Reader et bonnes pratiques

Pour prévenir autant que possible les attaques exploitant le format PDF, le CERT-FR préconise d'utiliser les options suivantes afin d'améliorer la sécurisation d'Adobe Reader :

- "Gestionnaire des approbations ->Autoriser l'ouverture de pièces jointes non PDF dans des applications externes" : doit être décochée ;
- "JavaScript ->Activer Adobe JavaScript" doit être décochée ;
- "Protection (renforcée) ->Activer la protection renforcée" doit être coché ;
- "Protection (renforcée) ->Créer un fichier journal" doit être coché ;
- "Générales ->Activer le mode protégé au démarrage" doit être coché ;
- "Générales ->Créer un fichier journal en mode protégé" doit être coché.

A noter qu'il est impossible d'interdire complètement l'utilisation de JavaScript ou l'ouverture de pièces jointes par ce biais, puisqu'une fenêtre sera systématiquement présentée à l'utilisateur, lui demandant s'il désire ou non utiliser ces fonctionnalités lorsqu'un document le nécessite. Cette fenêtre outrepassera alors temporairement la politique par défaut pour le document en cours de lecture.

Comme pour tout autre type de fichiers, il est recommandé de n'accepter et de n'ouvrir que les documents provenant de personnes ou d'entités de confiance. Ainsi, l'exécution éventuelle de JavaScript et la possible ouverture de fichiers embarqués dans ces documents ne seront réalisées que de manière ponctuelle sur les seuls fichiers pour lesquels cela est censé être légitime et nécessaire. Il est donc essentiel de sensibiliser l'utilisateur quant aux risques que présente le format PDF.

De plus, la mise à jour régulière des lecteurs de document, des systèmes d'exploitation et des antivirus, ainsi que l'installation de mécanismes de sécurité tel qu'EMET permettront de réduire l'exposition aux failles applicatives des stations de travail.

Enfin, la prévisualisation de document dans l'explorateur de fichiers et dans Outlook, ainsi que l'utilisation d'ActiveX pourra être désactivée afin de réduire le risque de compromission.

Rappel des avis et alertes émis

Depuis fin 2012, le format PDF a fait l'objet des avis et alertes suivants :

- Avis CERTA-2014-AVI-018 :
  http://www.cert.ssi.gouv.fr/site/CERTA-2014-AVI-018/
- Avis CERTA-2013-AVI-558 :
  http://www.cert.ssi.gouv.fr/site/CERTA-2013-AVI-558/
- Avis CERTA-2013-AVI-510 :
  http://www.cert.ssi.gouv.fr/site/CERTA-2013-AVI-510/
- Avis CERTA-2013-AVI-310 :
  http://www.cert.ssi.gouv.fr/site/CERTA-2013-AVI-310/
- Avis CERTA-2013-AVI-050 :
  http://www.cert.ssi.gouv.fr/site/CERTA-2013-AVI-050/
- Avis CERTA-2013-ALE-002 :
  http://www.cert.ssi.gouv.fr/site/CERTA-2013-ALE-002/
- Avis CERTA-2013-AVI-015 :
  http://www.cert.ssi.gouv.fr/site/CERTA-2013-AVI-015/
- Avis CERTA-2012-AVI-017 :
  http://www.cert.ssi.gouv.fr/site/CERTA-2012-AVI-017/

3 - Dernière mise à jour Java : changement du niveau de sécurité par défaut

Le 14 janvier 2014, Oracle a publié un ensemble de correctifs de sécurité appelé « Critical Patch Update » qui a fait l'objet de l'avis CERTA-2014-AVI-030. Parmi les multiples correctifs concernant les produits Oracle, une mise à jour est disponible pour Java SE qui correspond à la version 7 Update 51.

L'application de cette mise à jour change la politique de sécurité par défaut, qui passe alors au niveau « high », ce qui a pour conséquence de renforcer l'authentification des appliquettes et la gestion de leurs permissions.

Renforcement de l'authentification

Les appliquettes doivent être signées par une autorité de certification reconnue par le poste de l'utilisateur. Il n'est pas possible de forcer l'exécution d'appliquettes non signées ou signées à l'aide d'un certificat non reconnu ou auto-signé.

Renforcement de la gestion des permissions

Une appliquette est constituée d'une archive JAR contenant les fichiers nécessaires à son fonctionnement. Depuis la version 7 Update 51, le fichier « META-INF/MANIFEST.MF » contenant les attributs « Permissions » et « Codebase » est devenu obligatoire sous peine de voir l'application bloquée. Voici un exemple minimal de ce fichier pour que l'appliquette puisse être lancée depuis le navigateur :

```
Manifest-Version: 1.0
Created-By: 1.7.0_51
Permissions: sandbox
Codebase: www.java.com java.com
```

Les deux premières lignes donnent la version du fichier MANIFEST.MF ainsi que la version de Java utilisée pour créer l'appliquette.

La troisième ligne précise les droits requis par l'appliquette. Les deux valeurs possibles sont « sandbox » et « all-permissions ». La valeur « sandbox » signifie que l'appliquette peut s'exécuter au sein d'un bac à sable de sécurité alors que la valeur « all-permissions » indique que l'appliquette doit accéder à des ressources systèmes.

La quatrième ligne permet de restreindre le lancement de l'appliquette à un nom de domaine précis, empêchant ainsi une personne de déployer une appliquette sur un domaine différent de celui d'origine.

Recommandations

Ces deux renforcements peuvent provoquer des dysfonctionnements au niveau des appliquettes Java non compatibles qu'il convient alors de faire évoluer.

Le CERT-FR recommande de déployer cette mise à jour pour bénéficier des derniers correctifs de vulnérabilité et de renforcement du niveau de sécurité par défaut, tout en prenant soin de valider la compatibilité avec les appliquettes Java utilisées au sein de votre organisme.

Documentation

- Avis CERTA-2014-AVI-030 :
  http://www.cert.ssi.gouv.fr/site/CERTA-2014-AVI-030/index.html
- Améliorations apportées par Java 7 Update 51 :
  http://java.com/en/download/faq/release_changes.xml
- Vulnérabilités corrigées par Java 7 Update 51 :
  http://www.oracle.com/technetwork/topics/security/cpujan2014-1972949.html#AppendixJAVA
- Détails concernant la nouvelle politique de sécurité par défaut de Java :
  http://www.java.com/en/download/help/java_blocked.xml
- Détails des attributs constituant le fichier « MANIFEST.MF » :
  http://docs.oracle.com/javase/7/docs/technotes/guides/jweb/manifest.html

4 - Rappel des avis émis

Dans la période du 17 au 23 janvier 2014, le CERT-FR a émis les publications suivantes :

- CERTFR-2014-AVI-036 : Multiples vulnérabilités dans les produits VMware
- CERTFR-2014-AVI-037 : Multiples vulnérabilités dans Drupal
- CERTFR-2014-AVI-038 : Multiples vulnérabilités dans Moodle
- CERTFR-2014-AVI-039 : Multiples vulnérabilités dans les produits Citrix
- CERTFR-2014-AVI-040 : Multiples vulnérabilités dans Cisco TelePresence

Gestion détaillée du document

24 janvier 2014 version initiale.