Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 30 août 2013
N° CERTA-2013-ACT-035

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2013-ACT-035

1 Courriels malveillants exploitant des vulnérabilités connues

Le CERTA observe en continu des tentatives d'attaques par courriel qui cherchent à exploiter des vulnérabilités connues et corrigées. Ces courriels contiennent en pièce-jointe des charges malveillantes qui peuvent être compressées (notamment lorsqu'il s'agit d'un exécutable).

Les formats exploités par les attaquants correspondent aux formats les plus usités tels que Word, Excel ou PDF. Ainsi, entre 2011 et 2012, de nombreux documents Word et documents PDF visant à exploiter respectivement la CVE-2010-3333 et la CVE-2010-0188 ont été utilisés par des attaquants. Récemment, le CERTA a pu constater l'envoi de nombreux documents Excel visant à exploiter la vulnérabilité CVE-2012-0158.

Dans ces tentatives d'attaques, les attaquants utilisent des couriels et des noms de pièces-jointes génériques comme l'envoi d'un curriculum vitae ou le suivi d'une commande. L'adresse de l'émetteur est généralement usurpée ou correspondant à un compte de webmail. Il a également été observé des cas où l'attaquant reprend des sujets de l'actualité pour amener l'utilisateur à ouvrir le fichier joint malveillant.

Ces attaques visent des systèmes non à jour et à faible hygiène informatique, qui sont malheureusement encore trop souvent rencontrés. Il est donc indispensable pour s'en prémunir de s'assurer de la bonne mise à jour de l'intégralité du parc informatique. La mise en place de stratégie de restriction logicielles (SRP) ou d'AppLocker à partir de Windows 7 permettent aussi de se protéger efficacement contre ce type d'attaque.

Documentation

- Guide de configuration des stratégies de restriction logicielles :
  http://technet.microsoft.com/library/cc163080.aspx
- Guide de configuration de AppLocker :
  http://technet.microsoft.com/library/dd723678.aspx
- Guide d'hygiène informatique :
  http://www.ssi.gouv.fr/IMG/pdf/guide_hygiene_informatique_anssi.pdf
- Avis du CERTA concernant la CVE-2010-3333 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-543
- Avis du CERTA concernant la CVE-2012-0158 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-206
- Avis du CERTA concernant la CVE-2010-0188 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-081

2 Recrudescence des codes d'exploitation dans Oracle Java 6

Lors de la dernière mise à jour Java 7 update 25, de nombreuses vulnérabilités ont été corrigées dans le composant Java2D. Certaines de ces vulnérabilités sont aussi présentes dans la version 6 de Java. Depuis avril 2013, Oracle ne délivre plus de mise à jour et de correctif de sécurité gratuits pour Java SE version 6. Les vulnérabilités en question n'ont donc pas été corrigées pour la version 6 de Java et entraînent une recrudescence des codes d'exploitation ciblant cette version de Java encore largement employée.

De plus, de nombreux kits d'exploitation ont déjà intégré les codes d'exploitation et sont activement et massivement utilisés. Le CERTA incite donc à migrer au plus vite vers une version supportée de Java (version 7).

D'une manière générale, le CERTA recommande la plus grande vigilance sur la fin de support des versions de produits utilisés, afin de pouvoir anticiper les migrations nécessaires pour continuer à disposer des produits tenus à jour par les editeurs. Nous recommandons d'utiliser systématiquement la derniere version stable des produits et de veiller à la bonne mise à jour des correctifs de sécurité.

Documentation

- Oracle Java SE Support Roadmap :
  http://www.oracle.com/technetwork/java/eol-135779.html
- Les systèmes et logiciels obsolètes :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-003/

3 Traitement des contenus hétérogènes SSL dans les navigateurs

La mise à jour récente de Firefox en version 23 introduit une fonctionnalité déjà présente dans les dernières versions d'Internet Explorer et de Chrome : le blocage des données fournies par HTTP sur les pages HTTPS.

Lorsqu'un utilisateur navigue en utilisant le protocole HTTP sur TLS (*https*), la page HTML fournie peut référencer des ressources pointées par des liens en HTTP. Ce type de comportement pose plusieurs problèmes de sécurité, entre autres :

- un attaquant pouvant réaliser une attaque de l'homme du milieu (*man in the middle*) peut aisément remplacer des contenus actifs chargés *via* HTTP : par exemple un code *Javascript* d'analyse statistique pourrait être remplacé par un code malveillant exfiltrant les mots de passe des utilisateurs ;
- certaines ressources peuvent être chargées en spécifiant un *Cookie*, si celui-ci n'a pas été marqué par l'application Web comme *secure*, c'est-à-dire comme devant être transmis uniquement sur un canal sécurisé.

Firefox fait pour l'instant la distinction entre les contenus "actifs" et "passifs". Les contenus dits "actifs" sont ceux qui permettent de modifier le comportement du navigateur : scripts, feuilles de style, cadres, etc. Contrairement aux contenus "passifs", qui sont autorisés, les contenus "actifs" sont tout simplement bloqués lorsqu'ils sont chargés de manière non sécurisée et une icône de bouclier gris est présentée dans la barre d'adresse.

Chrome et Internet Explorer utilisent la même approche, même si quelques détails diffèrent.

Ces évolutions renforcent la sécurité des navigateurs Web, mais certains sites utilisant des contenus mixtes HTTP et HTTPS peuvent alors déclencher des alertes ou présenter des dysfonctionnements.

Le CERTA recommande aux éditeurs de sites de s'assurer que leurs pages HTTPS ne référencent pas de contenu HTTP et recommande aux utilisateurs de ne pas autoriser le chargement des contenus bloqués par les navigateurs.

Documentation

- Mozilla : Mixed Content Blocking Enabled in Firefox 23 :
  https://blog.mozilla.org/tanvi/2013/04/10/mixed-content-blocking-enabled-in-firefox-23/
- Chromium : Ending mixed scripting vulnerabilities :
  http://blog.chromium.org/2012/08/ending-mixed-scripting-vulnerabilities.html
- Internet Explorer 8 Mixed Content Handling :
  http://msdn.microsoft.com/en-us/library/ee264315(v=vs.85).aspx

4 Rappel des avis émis

Dans la période du 23 au 29 août 2013, le CERTA a émis les publications suivantes :

- CERTA-2013-AVI-492 : Vulnérabilité dans VMware Workstation
- CERTA-2013-AVI-493 : Multiples vulnérabilités dans RealNetworks realPlayer
- CERTA-2013-AVI-494 : Multiples vulnérabilités dans le noyau Linux de Red Hat
- CERTA-2013-AVI-495 : Multiples vulnérabilités dans Roundcube Webmail
- CERTA-2013-AVI-496 : Multiples vulnérabilités dans Citrix XenClient XT
- CERTA-2013-AVI-497 : Vulnérabilité dans Cisco Secure Access Control Server

Gestion détaillée du document

30 août 2013 version initiale.