Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 08 novembre 2013
N° CERTA-2013-ACT-045

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2013-ACT-045

1 - Vulnérabilité critique dans les produits Microsoft

Cette semaine, le CERTA a diffusé l'alerte CERTA-2013-ALE-007 concernant une vulnérabilité majeure dans les produits Microsoft. Cette vulnérabilité est désormais publique et largement exploitée par les attaquants.

Cette vulnérabilité est un dépassement de tampon dans le tas dans le composant GdiPlus de Microsoft, en charge notamment du rendu graphique des images TIFF. Elle permet une exécution de code arbitraire à distance au moyen d'un fichier embarquant une image au format TIFF spécialement conçue. Ce fichier peut être intégré dans un document Microsoft Office, une page Web ou un message électronique.

La vulnérabilité touche les versions 2003, 2007 et 2010 de Microsoft Office, quel que soit le système d'exploitation Microsoft Windows installé. De plus, les installations de Microsoft Windows Vista et Server 2008 sont également vulnérables, même si la suite Office n'est pas installée.

Différents codes d'exploitation sont déjà présents dans la nature sous la forme d'un document Word spécialement conçu. Pour contourner la protection ASLR, ils utilisent un contrôle ActiveX permettant de remplir le tas. En ce qui concerne la fonctionnalité DEP, deux types de contournement ont été constatés :

- le premier type de contournement utilise une bibliothèque chargée dans une zone fixe du processus pour effectuer le ROP (Return-Oriented Programming);
- le deuxième type de contournement, un peu plus original, force l'utilisation de la bibliothèque VBE6.DLL. Ce module, lors de son chargement, appelle la fonction ntdll!ZwSetInformationProcess pour désactiver la protection DEP sur le processus courant. Cet appel est utilisé à des fins de rétro compatibilité.

Microsoft a publié un correctif provisoire (cf. bulletin d'alerte). Le CERTA recommande l'application de ce correctif dès que possible. De plus, le CERTA encourage l'utilisation des dernières versions supportées des produits Microsoft et de lire le bulletin d'actualité numéro 42 (CERTA-2013-ACT-042) sur la protection ASLR.

Documentation

- Bulletin d'alerte nunéro 7 du 6 novembre 2013 du CERTA
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-ALE-007/index.html
- Microsoft Windows et Address Space Layout Randomization
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-ACT-042/index.html

2 - Bonnes pratiques lors de l'installation d'un logiciel

Il ressort des incidents traités par le CERTA que l'installation de logiciels sans vérifications préalables est régulièrement à l'origine de la compromission de postes de travail ou de serveurs.

Certaines précautions doivent être prises afin de garantir l'innocuité des logiciels installés sur un poste en production :

- le téléchargement d'un logiciel ou de son code source doit être réalisé, si possible, sur le site original de l'éditeur. En effet, de nombreux sites de téléchargement ajoutent à l'installation des programmes à vocation publicitaire ou des fonctionnalités non désirées (exemple : *barres d'outils*), qui peuvent faire l'objet de vulnérabilités ;
- les fichiers doivent être soumis à un ou plusieurs antivirus à jour;
- l'intégrité des fichiers téléchargés (sources ou binaires) doit être vérifiée en s'assurant que les condensats (MD5, SHA1, etc.) sont identiques à ceux publiés sur le site de l'éditeur. De même, la présence d'une signature numérique valide et d'origine sure garantira que le contenu n'a pas été modifié.
- la procédure d'installation doit être suivie avec attention afin de clairement identifier les composants installés et les options activées.

Ces précautions sont d'autant plus importantes lorsqu'il s'agit d'installer des composants de sécurité (exemple : *OpenSSH*) ou des services sensibles (exemple : *Serveur Web*).

Lors du déploiement dans un environnement critique, des précautions supplémentaires peuvent s'avérer utiles comme, par exemple, l'analyse du code source original, afin de s'assurer que le programme ne contient aucune fonction malveillante, ou la compilation d'un binaire directement depuis le code source.

Certaines attaques rencontrées redirigent l'utilisateur vers un site malveillant, visuellement identique au site de l'éditeur. Il convient donc de s'assurer que l'adresse Internet de téléchargement correspond bien à celle de l'éditeur.

Documentation

- Guide d'hygiène informatique :
  http://www.ssi.gouv.fr/IMG/pdf/guide_hygiene_informatique_anssi.pdf
- Compromission de VSFTPD :
  http://www.certa.ssi.gouv.fr/site/CERTA-2011-ACT-027/CERTA-2011-ACT-027.html
- Une porte dérobée dans le code source de phpMyAdmin :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-ACT-039/CERTA-2012-ACT-039.html

3 - Amélioration de la gestion des greffons applicatifs au sein des navigateurs Internet

Le CERTA a pu constater que dans un grand nombre d'incidents le point d'entrée utilisé était le navigateur Internet.

Dans le but de réduire les risques, les principaux éditeurs de navigateur Internet s'accordent sur l'évolution de la sécurité de leur logiciel en proposant de nouvelles options de sécurité, en particulier sur la gestion des greffons applicatifs (ex : *plug-ins, ActiveX*).

Ainsi, à partir de janvier 2014, Google dotera la nouvelle version de son navigateur Google Chrome d'une fonction permettant de désactiver tous les greffons basés sur NPAPI (Netscape Plug-in API), format couramment utilisé. Afin de ne pas handicaper les internautes, Google propose une liste de greffons autorisés en liste blanche : Silverlight, Unity, Google Earth, Google Talk, Facebook Video. Celle-ci peut être modifiée et être enrichie selon les besoins métier. Le plug-in Java reste désactivé par défaut. Cette nouvelle option constitue un complément à la fonction de sécurité « Safe Browsing » permettant d'alerter l'internaute si le site visité a été considéré comme malveillant par Google.

Il y a quelques jours, Mozilla a également doté la dernière version bêta 26 de son navigateur Internet Firefox d'une fonction de sécurité semblable, qui désactive par défaut tous les greffons installés, hormis les dernières versions des greffons Flash Player. La liste des greffons autorisés est également modifiable. Comme Google Chrome, une fonctionnalité déjà intégrée dans les dernières versions de Firefox apporte un complément de sécurité en alertant l'internaute s'il visite un site considéré comme malveillant (option de vérification des sites d'attaque et de contrefaçon).

Les versions supportées d'Internet Explorer intègrent une fonction de gestion des greffons. Internet Explorer en version 11, installé par défaut sur Microsoft Windows 8.1, intègre une fonction d'analyse des contrôles ActiveX, via Windows Defender, empêchant leur exécution s'ils sont considérés comme malveillants. Le filtre SmartScreen (base de données de sites malveillants) permet quant à lui d'alerter l'internaute si un site visité est considéré comme malveillant.

Le CERTA insiste donc sur la nécessité de mettre à jour son navigateur Internet et les greffons associés. Pour garantir une sécurité renforcée, il est par ailleurs conseillé de limiter les greffons autorisés et de paramétrer correctement leur configuration. Il est toutefois indispensable, avant d'effectuer les mises à jour sur un parc informatique, de les vérifier sur un environnement de test afin de s'assurer de leur stabilité et de leur compatibilité avec le système et les applications métier. Il est recommandé également de consulter l'article sur le détournement des greffons disponibles dans le bulletin d'actualité (CERTA-2013-ACT-004) ainsi que celui sur la protection des navigateurs contre les 0day (CERTA-2012-ACT-038).

Documentation

- Annonce de la nouvelle fonctionnalité de Google Chrome :
  http://blog.chromium.org/2013/09/saying-goodbye-to-our-old-friend-npapi.html
- Page de téléchargement de la dernière version Bêta de Firefox :
  http://www.mozilla.org/fr/firefox/beta/
- Nouveautés dans Windows 8.1:
  http://www.techspot.com/downloads/6059-microsoft-windows-81.html
- Bulletin d'actualité CERTA-2013-ACT-004 du 25 janvier 2013 « Détournement de greffons applicatifs (ou plug-ins) » :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-ACT-004
- Bulletin d'actualité CERTA-2012-ACT-038 du 21 septembre 2012 « Navigateurs Internet : prévention des attaques 0day » :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-ACT-038/

4 - Rappel des avis émis

Dans la période du 31 octobre au 07 novembre 2013, le CERTA a émis les publications suivantes :

- CERTA-2013-ALE-007 : Vulnérabilité dans un composant graphique de Microsoft
- CERTA-2013-AVI-614 : Vulnérabilité dans EMC Unisphere
- CERTA-2013-AVI-615 : Multiples vulnérabilités dans Cisco IOS XE Software
- CERTA-2013-AVI-616 : Multiples vulnérabilités dans Wireshark
- CERTA-2013-AVI-617 : Multiples vulnérabilités dans Xen
- CERTA-2013-AVI-618 : Vulnérabilité dans Cisco IOS Software
- CERTA-2013-AVI-619 : Vulnérabilité dans Cisco WAAS Mobile
- CERTA-2013-AVI-620 : Vulnérabilité dans Cisco TelePresence VX Clinical Assistant

Gestion détaillée du document

08 novembre 2013 version initiale.