Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 20 septembre 2013
N° CERTA-2013-ACT-038

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2013-ACT-038

1 Vulnérabilité critique dans Internet Explorer

Cette semaine, le CERTA a diffusé l'alerte CERTA-2013-ALE-006 concernant une vulnérabilité majeure dans Microsoft Internet Explorer. Des exploitations de cette vulnérabilité ont été constatées par Microsoft.

Cette faille permet d'exécuter du code arbitraire à distance. Il s'agit d'une utilisation après libération (Use-After-Free) dans la bibliothèque « mshtml.dll ». Cette bibliothèque, est le moteur de rendu de Microsoft Internet Explorer qui effectue le traitement du CSS, du HTML, et du Javascript des pages Web.

Le code d'exploitation de cette faille, développé en « javascript », utilise la bibliothèque « hxds.dll » pour contourner la protection d'ASLR utilisée par défaut dans Internet Explorer.

Microsoft a publié un correctif provisoire (cf. bulletin d'alerte). Le CERTA recommande l'application de ce correctif provisoire dès que possible. Par ailleurs, dans l'attente du correctif final de Microsoft, le CERTA propose plusieurs recommandations dans le bulletin d'alerte CERTA-2013-ALE-006 visant à réduire les risques liés à la vulnérabilité.

Documentation

- Bulletin d'alerte CERTA-2013-ALE-006 Vulnérabilité dans Internet Explorer : http://www.certa.ssi.gouv.fr/site/CERTA-2013-ALE-006/index.html

2 Précisions autour des récentes mises à jour Microsoft Update/Windows Update

Lors de la mise à disposition des mises à jour Microsoft de septembre, plusieurs problèmes ont été rencontrés:
- certains correctifs restaient considérés comme "à installer", alors que leur installation était pourtant effective ;
- certains correctifs étaient applicables, mais non proposés via les produits de déploiement de Microsoft (Windows Server Update Services (WSUS) ou System Center Configuration Manager (SCCM)).

Après investigation, Microsoft a déterminé que les métadonnées des correctifs suivants étaient en cause:
- KB2760589 : Mise à jour de sécurité pour Microsoft Office SharePoint Server 2007 ;
- KB2760411 : Mise à jour de sécurité pour Microsoft Office 2007 suites ;
- KB2767913 : Mise à jour de sécurité pour Microsoft Office 2010 ;
- KB2810048 : Mise à jour de sécurité pour Excel 2003 ;
- KB2760583 : Mise à jour de sécurité pour Microsoft Office Excel 2007 ;

– KB2760590 : Mise à jour de sécurité pour Excel Viewer ;
– KB2760588 : Mise à jour de sécurité pour Microsoft Office 2007 suites ;
– KB2810009 : Mise à jour de sécurité pour Microsoft Office 2013 (version 64-bit) ;
– KB2553145 : Mise à jour de sécurité pour PowerPoint 2010 ;
– KB2553351 : Mise à jour de sécurité pour PowerPoint Viewer 2010 ;

l'algorithme de gestion des mises à jour ne parvenant pas à déterminer avec fiabilité si ces mises à jour étaient applicables ou appliquées.

Microsoft a depuis publié de nouveaux paramètres de détection corrigeant ces problèmes. Les correctifs restant, eux, inchangés.

Le CERTA recommande donc l'application cette nouvelle version sur l'ensemble des machines, y compris celles présentes sur les réseaux déconnectés.

Documentation

– Blog de Microsoft Office :
http://blogs.technet.com/b/office_sustained_engineering/archive/2013/09/12/september-2013-public-update-update-targeting-for-microsoft-update-wsus-and-sccm.aspx

3 Mises à jour Mozilla

Lors de la dernière mise à jour des produits Mozilla, dix-sept bulletins de sécurité ont été publiés.

Sept bulletins sont critiques pour l'éditeur, ils concernent :

– MFSA2013-76 cette mise à jour corrige plusieurs corruptions de mémoire dans les produits Mozilla, les plus graves pourraient permettre l'exécution de code à distance au moyen d'une page Web spécialement conçue ;
– MFSA2013-78 qui concerne la bibliothèque Almost Native Graphics Layer Engine (ANGLE). Cette mise à jour corrige une vulnérabilité de type débordement d'entier entraînant une corruption de mémoire dans la fonction « drawLineLoop ». Elle pourrait permettre l'exécution de code à distance si un utilisateur ouvrait une page Web spécialement conçue ;
– MFSA2013-79 qui concerne la gestion des feuille de style dans l'Animation Manager des produits Mozilla. Cette mise à jour corrige une vulnérabilité de type utilisation après libération (use after free) qui pourrait permettre l'exécution de code à distance, si un utilisateur affichait une page Web spécialement conçue ;
– MFSA2013-81 qui concerne la gestion des fomulaires HTML dans les produits Mozilla, cette mise à jour corrige une vulnérabilité de type utilisation après libération (use after free) qui pourrait permettre l'exécution de code à distance, si un utilisateur affichait une page Web spécialement conçue ;
– MFSA2013-89 qui concerne le composant « nsFloatManager » des produits Mozilla, cette mise à jour corrige une vulnérabilité de type débordement de tampon. Elle pourrait permettre l'exécution de code à distance, si un utilisateur affichait une page Web spécialement conçue ;
– MFSA2013-90 cette mise à jour corrige plusieurs corruptions de mémoire dans les produits Mozilla. La principale vulnérabilité est référencée par le CVE-2013-1735. Il s'agit d'une utilisation après libération (use after free) dans la fonction « mozilla::layout::ScollbarActivity ». Elle pourrait permettre une exécution de code à distance lors du défilement d'une image dans une page Web spécialement conçue ;
– MFSA2013-92 cette mise à jour corrige plusieurs corruptions de mémoire dans les produits Mozilla, les plus graves sont dues à des défauts dans le Garbage Collector des produits Mozilla. Elles pourraient permettre l'exécution de code à distance au moyen d'une page Web spécialement conçue.

Quatre bulletins sont considérés importants par l'éditeur, ils concernent :

– une vulnérabilité dans le moteur JavaScript des produits Mozilla (MFSA2013-82) ;
– une vulnérabilité dans le processus de vérification de signature lors des mises à jour des produits Mozilla (MFSA2013-083). Elle permet à un attaquant local de remplacer le contenu d'un fichier MAR (Mozilla ARchive) et donc de modifier un produit Mozilla lors de sa mise à jour.
– une vulnérabilité dans Mozilla Firefox (MFSA2013-87). Elle permettrait à un attaquant local de remplacer la bibliothèque dynamique de Firefox destinée au traçage d'élements graphiques GL (Graphics Library). Cela entraîne la possibilité d'injecter du code malveillant dans une instance de Firefox ;

– une vulnérabilité dans l'implémentation de XBL (XML Binding Language) dans les produits Mozilla (MFSA2013-88). Elle permet à un attaquant de provoquer un déni de service à distance au moyen d'une page Web spécialement conçue.

Mozilla rappelle que la plupart de ces vulnérabilités ne sont pas exploitables dans le produit Thunderbird car les langages de programmation interprétés tel que JavaScript sont désactivés dans les courriels.

Le CERTA recommande l'application de ces correctifs dès que possible et la mise à jour des logiciels embarquant les produits Mozilla.

Documentation

– Avis CERTA-2013-AVI-531 :
http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-531/

4 Le serveur HTTP d'Apache et les extensions de fichiers

Cet article a pour but d'éclairer la façon dont le serveur HTTP d'Apache (*httpd*) utilise les extensions de fichiers pour déterminer leur type de contenu. La méthode utilisée par Apache *httpd* peut, dans des cas particuliers, induire des risques de sécurité. Une configuration adéquate permet de limiter ces risques.

Dans la configuration d'Apache *httpd*, les correspondances entre extensions et types de contenu peuvent être spécifiées avec les directives suivantes :

– `TypesConfig` : permet de spécifier le chemin vers un fichier listant les correspondances par défaut entre extensions et types de contenu. C'est généralement un fichier nommé *mime.types*, pouvant être global au système d'exploitation, qui est utilisé ;
– `AddType` : permet de spécifier une correspondance, remplaçant une potentielle correspondance déjà présente dans le fichier spécifié par `TypesConfig`.

Lorsque les extensions sont déclarées par les directives citées ci-dessus, c'est l'extension connue la plus à droite dans un nom de fichier qui est prise en compte. Par exemple, les fichiers suivants sont considérés comme contenant du code PHP et sont donc exécutés par le serveur Web lorsqu'ils sont demandés :

```
test.php.unknown
test.unknown.php.unknown
```

Ce comportement est a priori sans risque lorsque les fichiers accessibles par le serveur Web sont totalement contrôlés. En revanche, couplé à une fonctionnalité de téléversement (*upload*) comme il en existe dans différents CMS (*Content Management System*), ce comportement peut devenir dangereux. En effet, s'il existe une extension autorisée à l'envoi par le CMS, mais non connue par Apache *httpd*, il peut être possible d'exécuter du code, comme du code PHP, sur le serveur.

Pour éviter que ce comportement soit abusé, il est possible de configurer Apache *httpd* en respectant les étapes suivantes :

1. retirer les correspondances pour PHP dans le fichier spécifié par `TypesConfig`. Si ce fichier est global au système, il est nécessaire d'évaluer l'impact de cette modification ;
2. retirer les correspondances pour PHP spécifiées par les directives `AddType` ou `AddHandler` ;
3. indiquer explicitement que l'extension PHP doit se trouver à la fin du nom de fichier lorsque l'interpréteur PHP est invoqué :

```
<FilesMatch \.php$>
    SetHandler php5-script
</FilesMatch>
```

Il est recommandé de configurer de cette manière toute extension jugée dangereuse.

A titre d'exemple, une vulnérabilité récemment corrigée dans *Joomla!*, dont il est question dans l'avis CERTA-2013-AVI-460, n'aurait pas pu être exploitée jusqu'à l'exécution de code si la configuration proposée ici avait été appliquée.

Notes : il convient de noter que les directives `AddHandler` ou `SetHandler` ont une priorité plus haute que les directives `TypesConfig` ou `AddType` et doivent être utilisées avec précaution. Pour plus de détails sur ces directives, il est conseillé de se référer à la documentation d'Apache *httpd*.

Documentation

- Documentation d'Apache *httpd* concernant les extensions de fichiers et les contenus :
  http://httpd.apache.org/docs/current/mod/mod_mime.html
- Avis CERTA-2013-AVI-460 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-460/
- Bulletin de sécurité *Joomla!* du 31 juillet 2013 :
  http://developer.joomla.org/security/news/563-20130801-core-unauthorised-uploads
- Recommandations publiées par l'ANSSI sur la sécurisation des sites Web :
  http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-des-applications-web/recommandations-pour-la-securisation-des-sites-web.html

5 Rappel des avis émis

Dans la période du 13 au 19 septembre 2013, le CERTA a émis les publications suivantes :

- CERTA-2013-ALE-006 : Vulnérabilité dans Microsoft Internet Explorer
- CERTA-2013-AVI-528 : Multiples vulnérabilités dans Apple Safari
- CERTA-2013-AVI-529 : Multiples vulnérabilités dans Apple OS X Mountain Lion
- CERTA-2013-AVI-530 : Multiples vulnérabilités dans Moodle
- CERTA-2013-AVI-531 : Multiples vulnérabilités dans les produits Mozilla
- CERTA-2013-AVI-532 : Multiples vulnérabilités dans Apple OS X Server
- CERTA-2013-AVI-533 : Vulnérabilité dans Cisco Prime Central
- CERTA-2013-AVI-534 : Multiples vulnérabilités dans Cisco Prime Data Center Network Manager
- CERTA-2013-AVI-535 : Vulnérabilité dans Apple iTunes
- CERTA-2013-AVI-536 : Multiples vulnérabilités dans Apple iOS
- CERTA-2013-AVI-537 : Vulnérabilité dans Apple Xcode

Gestion détaillée du document

20 septembre 2013 version initiale.