Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 11 janvier 2013
N° CERTA-2013-ACT-002

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2013-ACT-002

1 Vulnérabilité critique dans Oracle Java

Cette semaine le CERTA a diffusé l'alerte CERTA-2013-ALE-001, concernant une vulnérabilité majeure dans *Oracle Java*. La faille permet d'exécuter du code arbitraire à distance. Elle a été largement diffusée via une plateforme très connue d'attaque. Dans les cas où *Java* n'est pas nécessaire, le désactiver complètement est un bon moyen de réduire la surface d'attaque du poste. En revanche, si *Java* est requis pour certains sites ou applications métier, une solution peut consister à désactiver *Java* dans le navigateur principal et à utiliser un navigateur alternatif, dans lequel *Java* est activé pour consulter ces sites.

Vous trouverez ci-dessous des sections décrivant plusieurs méthodes pour désactiver *Java* dans différents environnements.

1.1 Instructions pour désactiver Java dans Windows

1. Fermer tout navigateur Internet ;
2. aller dans « Panneau de configuration », « Désinstaller un programme » ;
3. trouver *Java* dans la liste, le sélectionner et cliquer sur « Désinstaller ».

1.2 Instructions pour désactiver Java dans *Firefox*

1. Aller dans le menu « Outils » puis « Modules complémentaires » ;
2. choisir l'onglet « Plugins » ;
3. cliquer sur le bouton « Désactiver » pour les *plugins* en relation avec *Java*.

1.3 Instructions pour désactiver Java dans *Internet Explorer*

1. Aller dans le menu « Outils » puis « Gérer les modules complémentaires » ;
2. choisir « Barres d'outils et extensions» ;
3. désactiver tous les *plugins* en relation avec *Java*.

1.4 Instructions pour désactiver Java dans *Google Chrome*

1. Saisir « chrome://plugins/ » dans la barre d'adresse ;
2. cliquer sur « Désactiver » pour le *plugin Java*.

1.5 Instructions pour désactiver Java dans *Safari*

1. Aller dans « Préférences » puis « Sécurité » ;
2. décocher *Java*.

1.6 Instructions pour désactiver Java dans *Opera*

1. Saisir « opera:plugins » dans la barre d'adresse ;
2. cliquer sur « Désactiver » pour les objets relatifs à *Java* dans la liste.

Documentation

– Alerte CERTA-2013-ALE-001 :
http://www.certa.ssi.gouv.fr/site/CERTA-2013-ALE-001/
– Bulletin d'actualité CERTA-2012-ACT-035 :
http://www.certa.ssi.gouv.fr/site/CERTA-2012-ACT-035/

2 Attaques « point d'eau » : un mode opératoire efficace

Depuis plusieurs années, l'ANSSI assiste des organisations confrontées à des attaquants utilisant un mode opératoire connu sous le nom de « point d'eau » (*watering hole* en anglais). Le nom de ce mode opératoire vient du fait que les attaquants qui l'utilisent se comportent comme les prédateurs qui, au lieu d'aller pourchasser le gibier dans la savane, l'attendent à côté d'un point d'eau.

En pratique, les attaquants compromettent, puis piègent, un ou plusieurs sites Web qu'ils présument fréquentés par les employés de leur cible. Puis, ils attendent que le poste d'un employé de leur cible visite un de ces sites et soit infecté pour en prendre le contrôle à distance et tenter de rebondir sur le réseau interne. Pour accélérer le processus, une fois le piège posé, les attaquants peuvent envoyer à des employés ciblés un courriel avec un lien pour les attirer vers le site piégé.

Fort logiquement, les sites compromis dans le cadre de telles attaques seront ceux en rapport avec les activités de la cible. Il peut s'agir de sites de *think tank*, de groupes de travail ou d'associations professionnelles dont fait partie la cible, mais aussi du propre site de la cible ou de celui d'un concurrent, d'un partenaire, d'une section syndicale ou du comité d'entreprise.

Pour les attaquants, une telle approche est intéressante, car elle permet de contourner les listes blanches mises en place par les cibles et peut conduire à la compromission de plusieurs cibles avec un seul piège. Par ce biais, les attaquants peuvent ainsi cibler des profils d'employés ou de secteurs entiers. De plus, les utilisateurs peuvent être moins vigilants lorsqu'ils visitent des sites qu'ils fréquentent régulièrement, comme le site de leur organisation, d'un partenaire ou d'un concurrent (l'exécution de scripts sera souvent activée par défaut pour ces sites).

Toutes les organisations opérant dans des secteurs stratégiques peuvent être victimes de ce mode opératoire du point d'eau, de plus en plus observé, en France comme ailleurs.

L'application des règles élémentaires de sécurité peut permettre de déjouer nombre d'attaques reposant sur ce mode opératoire : mise à jour et durcissement des postes de travail, sensibilisation des utilisateurs, mise en place de systèmes de détection de téléchargement d'exécutables, de scans de port sur le réseau interne, de flux d'exfiltration, ...

Face à cette menace, une attention particulière devra par ailleurs être portée sur la sécurité des sites Web de l'organisation et des serveurs les hébergeant, qu'ils soient ou non sous le contrôle de la DSI. Dans de grandes structures, il n'est en effet pas rare que des sites évènementiels, de communication ou de comité d'entreprise soient externalisés, et ne bénéficient alors pas forcément de la même rigueur dans le contrôle de leur sécurité.

L'ANSSI propose plusieurs guides utiles sur ces sujets. Ils sont consultables à l'adresse suivante :
http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/

3 Caractéristiques et limitations des Fix It de Microsoft

Le 31 décembre 2012 *Microsoft* a publié une contre-mesure provisoire dite *Fix It*, concernant une vulnérabilité dans *Internet Explorer 8*. Le CERTA profite de cette diffusion pour rappeler quelles sont les caractéristiques et les limitations liées à ces types de contre-mesures.

La publication d'un *Fix It* est une réponse d'urgence à une vulnérabilité, ou à un défaut de conception, activement utilisé par des tiers afin d'attaquer des systèmes d'informations. L'objectif premier est de bloquer le plus rapidement possible les codes d'exploitation existants, sans pour autant altérer la stabilité du système. Pour cela, *Microsoft* peut modifier des valeurs et des clés dans la base de registre, ou remanier des binaires à chaud au moyen de protocoles de modification temporaire des exécutables (*Shims*). Ces *Shims* injectent un exécutable DLL dans les processus concernés pour changer une partie du code. Les systèmes bénéficiant d'un *Fix It* réduisent les risques liés à un code d'exploitation identifié sans pour autant y remédier en totalité.

Le *Fix It* répond donc à une problématique donnée, à un instant donné. Si la surface d'attaque évolue avec le temps, le *Fix It* pourrait ne pas répondre à ces nouvelles menaces. De plus, il ne s'applique pas toujours à toutes les versions de Windows. Il convient donc d'avoir un système déjà à jour pour bénéficier de sa protection.

Par ailleurs, si l'application des contre-mesures provisoires est importante pour la sécurité d'un système d'information, elle doit être évaluée et préparée pour éviter toute régression du système d'information. Le CERTA rappelle enfin qu'un *Fix It* est une réponse d'urgence pour limiter à moindre coût la surface d'exploitation d'une vulnérabilité, dans l'attente de sa correction par l'éditeur.

4 Mise à jour mensuelle Microsoft

Lors de la mise à jour mensuelle de Microsoft, sept bulletins de sécurité ont été publiés.

Deux bulletins sont considérés comme critiques :

- MS13-001 qui concerne les composants du spouleur d'impression Windows, cette mise à jour corrige une vulnérabilité permettant à un attaquant, à l'aide d'une tâche d'impression spécialement conçue, d'exécuter du code arbitraire à distance ;
- MS13-002 qui concerne Microsoft XML Core Services, cette mise à jour corrige deux vulnérabilités permettant à un attaquant, à l'aide de pages Web spécialement conçues, d'exécuter du code arbitraire à distance.

Cinq bulletins sont considérés comme importants, ils concernent :

- des vulnérabilités dans System Center Operations Manager de Microsoft (MS13-003) ;
- des vulnérabilités dans .NET Framework (MS13-004) ;
- une vulnérabilité dans les pilotes en mode noyau de Windows (MS13-005) ;
- une vulnérabilité dans Microsoft Windows (MS13-006) ;
- une vulnérabilité dans le protocole Open Data (MS13-007).

Microsoft n'a pas constaté d'exploitation de ces vulnérabilités avant la publication de ces correctifs. Le CERTA recommande l'application de ces correctifs dès que possible.

Documentation

- Synthèse des bulletins de sécurité Microsoft du mois de janvier 2013 :
  http://technet.microsoft.com/fr-fr/security/bulletin/ms13-jan
- Avis CERTA-2013-AVI-007 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-007/
- Avis CERTA-2013-AVI-008 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-008/
- Avis CERTA-2013-AVI-009 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-009/
- Avis CERTA-2013-AVI-010 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-010/
- Avis CERTA-2013-AVI-011 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-011/
- Avis CERTA-2013-AVI-012 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-012/
- Avis CERTA-2013-AVI-013 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-013/

5 Rappel des avis émis

Dans la période du 04 au 10 janvier 2013, le CERTA a émis les publications suivantes :

- CERTA-2013-ALE-001 : Vulnérabilité dans Oracle Java
- CERTA-2013-AVI-004 : Vulnérabilité dans RPM Package Manager
- CERTA-2013-AVI-005 : Vulnérabilité dans EMC NetWorker
- CERTA-2013-AVI-006 : Vulnérabilité dans ProFTPD
- CERTA-2013-AVI-007 : Vulnérabilité dans les composants du spouleur d'impression Windows
- CERTA-2013-AVI-008 : Multiples vulnérabilités dans System Center Operations Manager de Microsoft
- CERTA-2013-AVI-009 : Vulnérabilité dans Microsoft NET Framework
- CERTA-2013-AVI-010 : Vulnérabilité dans les pilotes en mode noyau de Windows
- CERTA-2013-AVI-011 : Multiples vulnérabilités dans Microsoft XML Core Services
- CERTA-2013-AVI-012 : Vulnérabilité dans Microsoft Windows
- CERTA-2013-AVI-013 : Multiples vulnérabilités dans Microsoft NET Framework
- CERTA-2013-AVI-014 : Vulnérabilité dans Adobe Flash Player
- CERTA-2013-AVI-015 : Multiples vulnérabilités dans Adobe Reader et Acrobat
- CERTA-2013-AVI-016 : Multiples vulnérabilités dans HP OpenVMS
- CERTA-2013-AVI-017 : Multiples vulnérabilités dans Sybase Adaptive Server Entreprise
- CERTA-2013-AVI-018 : Vulnérabilité dans le système SCADA Siemens ProcessSuite
- CERTA-2013-AVI-019 : Vulnérabilité dans Cisco Prime LAN Management Solution
- CERTA-2013-AVI-020 : Vulnérabilité dans Cisco Unified IP Phone
- CERTA-2013-AVI-021 : Vulnérabilité dans le système SCADA RuggedCom
- CERTA-2013-AVI-022 : Multiples vulnérabilités dans les produits Mozilla

Durant la même période, les publications suivantes ont été mises à jour :

- CERTA-2012-ALE-007-001 : Vulnérabilité dans MySQL (fermeture de l'alerte, suite à la correction silencieuse par l'éditeur)
- CERTA-2012-ALE-009-001 : Vulnérabilité dans les pilotes NVidia (ajout du correctif éditeur, suppression du contournement provisoire)
- CERTA-2012-ALE-010-002 : Vulnérabilité dans Internet Explorer (ajout d'une précision sur le « Fix it » dans les contournements provisoires)

Gestion détaillée du document

11 janvier 2013 version initiale.