Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 31 août 2012
N° CERTA-2012-ACT-035

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2012-ACT-035

Gestion du document

Référence	CERTA-2012-ACT-035
Titre	Bulletin d'actualité CERTA-2012-ACT-035
Date de la première version	31 août 2012
Date de la dernière version	–
Source(s)	
Pièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 Vulnérabilités critiques dans Java corrigées par Oracle

Cette semaine, le CERTA a diffusé une alerte CERTA-2012-ALE-005 concernant une vulnérabilité dans *Java*. L'éditeur Oracle a depuis publié des correctifs pour les versions 1.6 et 1.7 de *Java*, couvrant notamment les vulnérabilités sur lesquelles portait notre alerte.

Ces derniers jours, des codes d'exploitation ont rapidement circulé sur l'Internet et sont actuellement utilisés par un nombre grandissant d'attaquants. Le CERTA recommande donc fortement d'installer les correctifs le plus rapidement possible (voir la section Documentation).

Cet événement doit être l'occasion de s'interroger sur l'intérêt d'avoir *Java* installé sur son poste, à l'instar de tout autre module tiers.

Dans les cas où *Java* n'est pas nécessaire, le désactiver complètement est un bon moyen de réduire la surface d'attaque du poste. Dans les cas où *Java* serait requis pour certains sites ou applications identifiés, une solution est de le désactiver dans le navigateur principal et de réserver un navigateur alternatif, où *Java* serait activé pour consulter ces sites.

Le CERTA rappelle qu'il est possible, suite à des mises à jour, d'avoir différentes versions de *Java* installées sur un même poste. Il convient de supprimer les versions qui ne sont pas utilisées.

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

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.

1.7 Documentation

- Alerte CERTA-2012-ALE-005 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-ALE-005/index.html
- Correctifs pour Java 7 (Java 7 Update 7):
  http://www.oracle.com/technetwork/java/javase/downloads/jre7u7-downloads-1836441.html
- Correctifs pour Java 6 (Java 6 Update 35):
  http://www.oracle.com/technetwork/java/javase/downloads/jre6u35-downloads-1836473.html

2 Défense en profondeur des SI : un principe à ne pas oublier

Un site web d'une entité administrative créé pour informer les usagers n'a pu assurer son service pendant quelques jours. Le contenu utile est devenu inaccessible suite à une modification du site par des intrus.

Un compte FTP était autorisé à opérer des modifications sur le site. Il était utilisé par un seul adminsitrateur et le mot de passe était fort. Le mot de passe a été capté par un moyen non déterminé, mais pas par une attaque par dictionnaire ou par recherche exhaustive. L'absence de plusieurs lignes de défense indépendantes a dès lors permis à l'agresseur d'atteindre son but sans difficulté.

Dans le cas présent, le filtrage sur l'adresse IP des accès au serveur FTP aurait rendu la tâche plus complexe pour l'agresseur. Indépendamment, l'utilisation d'un protocole tel SFTP ou SSH à la place de FTP, ou un tunnel IPSec, aurait diminué la vulnérabilité du mot de passe à l'écoute.

Le CERTA rappelle que la protection d'un système d'information ne peut reposer sur une seule ligne de défense.

La remise en état du site concerné a bien sûr pris en compte ce principe.

Documentation

– Mémento «La défense en profondeur appliquée aux systèmes d'information » du 19 juillet 2004
http://circulaire.legifrance.gouv.fr/pdf/2009/04/cir_2014.pdf

3 Rappel des avis émis

Dans la période du 24 août 2012 au 30 août 2012, le CERTA a émis les publications suivantes :

– CERTA-2012-ALE-005 : Vulnérabilité dans Oracle Java
– CERTA-2012-AVI-465 : Vulnérabilité dans le système SCADA RUGGEDCOM Rugged Operating System
– CERTA-2012-AVI-466 : Vulnérabilité dans les produits EMC ApplicationXtender
– CERTA-2012-AVI-467 : Multiples vulnérabilités dans les produits Mozilla
– CERTA-2012-AVI-468 : Multiples vulnérabilités dans Symantec Messaging Gateway
– CERTA-2012-AVI-469 : Vulnérabilité dans HP iNode Management Center
– CERTA-2012-AVI-470 : Vulnérabilité dans HP Intelligent Management Center
– CERTA-2012-AVI-471 : Vulnérabilité dans EMC Cloud Tiering Appliance
– CERTA-2012-AVI-472 : Vulnérabilités dans IBM Infosphere Guardium

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

– CERTA-2012-ALE-005-001 : Vulnérabilité dans Oracle Java (ajout de la solution).

4 Actions suggérées

4.1 Respecter la politique de sécurité

La Politique de Sécurité des Systèmes d'Information (PSSI) est l'ensemble formalisé dans un document applicable, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection des systèmes d'information de l'organisme. Elle traduit la reconnaissance officielle de l'importance accordée par la direction générale de l'organisme à la sécurité de ses systèmes d'information. D'une manière générale, elle contient une partie relative aux éléments stratégiques de l'organisme (périmètre, contexte, enjeux, orientations stratégiques en matière de SSI, référentiel règlementaire, échelle de sensibilité, besoins de sécurité, menaces) et une partie relative aux règles de sécurité applicables. Elle constitue donc une traduction concrète de la stratégie de sécurité de l'organisme.

Quoique puisse suggérer ce document, la politique de sécurité en vigueur dans votre service doit primer.

Cette section précise néanmoins quelques mesures générales de nature à vous prémunir contre les agressions décrites dans ce document. En effet, la sécurité des systèmes d'information ne repose pas exclusivement sur des outils, mais aussi sur une organisation et des politiques.

4.2 Concevoir une architecture robuste

A la lumière des enseignements tirés de ce qui a été présenté dans les bulletins d'actualité, il convient de vérifier que les applications mises en oeuvre (ou à l'étude) ont une architecture qui résiste aux incidents décrits.

4.3 Appliquer les correctifs de sécurité

Le CERTA recommande l'application des correctifs de sécurité.

4.4 Utiliser un pare-feu

L'application des correctifs sur un parc informatique important n'est probablement pas immédiate. Un pare-feu correctement configuré peut retenir certaines attaques informatiques le temps d'appliquer les correctifs. Cependant un pare-feu peut donner une illusion de protection. Cette protection est brisée par la moindre introduction d'un ordinateur nomade dans la partie protégée. On remarque qu'il y a de nombreux paquets rejetés à destination de ports légitimement utilisés par des applications de prise de main à distance. La téléadministration correspond à une demande qui grandit avec la taille du parc à gérer. Les paquets rejetés montrent le risque associé à ce type d'application. Ce risque peut être amoindri par l'usage correct d'un pare-feu.

4.5 Analyser le réseau

De nombreux paquets rejetés étudiés correspondent aux ports ouverts par divers virus/vers/chevaux de Troie. Si votre politique de sécurité autorise le balayage des ports ouverts sur les postes de travail ou les serveurs, il peut s'avérer utile de le faire régulièrement afin de découvrir les machines potentiellement contaminées avant qu'un intrus ne le fasse à votre place.

L'analyse des journaux de votre pare-feu est une source pertinente d'informations pour la sécurité de votre réseau et de vos systèmes. Cela peut vous aider à anticiper des incidents en remarquant par exemple des activités anormales. Le CERTA peut vous aider dans ce travail d'analyse.

4.6 Réagir aux incidents de sécurité

Organisez-vous pour réagir aux incidents de sécurité, en particulier, pour assurer une certaine continuité dans les équipes d'administration et de sécurité.

Le CERTA a pour mission de vous aider à répondre aux incidents de sécurité informatique.

Ne traitez pas les dysfonctionnements des machines à la légère. Dans certains incidents dans lesquels le CERTA intervient, les administrateurs des machines font spontanément part de petits dysfonctionnements inexpliqués et d'apparence anodine qui s'avèrent, au cours de l'analyse, être liés à un incident majeur de sécurité. N'hésitez pas à prendre contact avec le CERTA si vous constatez de l'activité sur les ports décrits ci-dessus.

4.7 Former et sensibiliser les utilisateurs

La sécurité d'un système d'information doit reposer sur une approche de défense en profondeur. Cela signifie, entre autres choses, que l'utilisateur est partie prenante de la sécurité. Sa vigilance, son niveau de formation et de sensibilisation participent à la sécurité du système. C'est pourquoi il est essentiel de prévoir des séances de formation et de sensibilisation des utilisateurs, acteurs de la sécurité. Pour vous aider dans ces actions, l'ANSSI dispose d'un centre de formation :

http://www.ssi.gouv.fr/site_rubrique62.html

Gestion détaillée du document

31 août 2012 version initiale.