Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 19 avril 2013
N° CERTA-2013-ACT-016

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2013-ACT-016

1 Correctifs Oracle

Oracle a publié cette semaine des mises à jour corrigeant de nombreuses vulnérabilités dans certains de ses produits tels que Java, MySQL, Oracle Database, Solaris, GlassFish, etc.

Les vulnérabilités les plus critiques concernent les trois premiers produits sus-cités et permettent l'exécution de code arbitraire à distance ou la divulgation de données confidentielles par un attaquant.

A noter que des codes d'exploitation pour Java qui permettent d'exécuter du code arbitraire à distance (versions antérieures à 1.7.21) sont largement diffusés sur Internet.

De nombreuses solutions tiers utilisent des composants Oracle. Des mises à jour de ces solutions sont donc à prévoir.

Le CERTA recommande l'application de ces correctifs dès que possible.

Documentation

- Bulletin de sécurité Oracle JavaCPUApr2013 du 16 avril 2013 :
  http://www.oracle.com/technetwork/topics/security/javacpuapr2013-1928497.html
- Bulletin de sécurité Oracle CPUApr2013 du 16 avril 2013 :
  http://www.oracle.com/technetwork/topics/security/cpuapr2013-1899555.html

2 Rappel sur la fin de support de Oracle Java 6 et Microsoft Windows XP

2.1 Fin de support Oracle Java 6

Depuis février 2013, Oracle ne délivre plus de mise à jour et de correctif de sécurité gratuits pour Java SE version 6. Oracle a démarré en décembre 2012 un processus de mise à jour automatique vers Java 7 pour les versions Windows 32-bit. Toutefois, de nombreuses utilisations de Java version 6 sont encore fréquemment rencontrées.

Le CERTA incite donc les administrateurs et les développeurs Java version 6 qui ne l'auraient pas déjà fait à migrer au plus vite vers une version supportée de Java (version 7).

2.2 Fin de support Microsoft Windows XP

Microsoft a planifié l'arrêt du support de Microsoft Windows XP en avril 2014. A cette date, l'éditeur cessera d'assurer la publication de correctifs de sécurité pour Windows XP, y compris en cas de découverte d'une vulnérabilité critique.

De nombreux systèmes utilisant Microsoft Windows XP sont aujourd'hui encore en service dans les administrations et les entreprises.

Le CERTA attire l'attention sur la nécessité d'anticiper dès à présent une migration des systèmes fonctionnant sous Windows XP vers un système d'exploitation dont la pérennité des mises à jour de sécurité pourra être assurée après cette date.

2.3 Anticipation des obsolescences logicielles

D'une manière générale, le CERTA recommande la plus grande vigilance sur la date d'échéance 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

- Java 6 Auto-Update to Java 7 :
  http://www.oracle.com/technetwork/java/javase/documentation/autoupdate-1667051.html
- Oracle Java SE Support Roadmap :
  http://www.oracle.com/technetwork/java/eol-135779.html
- Microsoft Support Lifecycle :
  http://support.microsoft.com/lifecycle/
- Les systèmes et logiciels obsolètes :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-003/

3 Recommandations de sécurité relatives aux environnements d'exécution Java sur les postes de travail Microsoft Windows

Une note technique de recommandations sur la sécurisation de Java sur les postes Microsoft Windows a été publiée par l'ANSSI le 19 avril 2013.

La technologie Java est aujourd'hui très répandue et utilisée par de nombreuses applications. Ces applications se présentent souvent sous la forme d'appliquettes (applets) exécutées depuis des clients légers (navigateurs Web) mais peuvent aussi être des applications lourdes installées sur les postes utilisateurs.

Comme tout composant logiciel utilisé pour la navigation Web, les environnements d'exécution Java sont une cible privilégiée des attaquants et font régulièrement l'actualité pour leurs vulnérabilités.

Le CERTA recommande la lecture de cette note technique et l'application des recommandations qu'elle contient sur tous les postes de travail Microsoft Windows.

Documentation

- Recommandations de sécurité relatives à Java :
  http://www.ssi.gouv.fr/recos-securite-poste-java

4 Recommandations pour un usage sécurisé d'(Open)SSH

Une note technique de recommandations sur l'utilisation d'OpenSSH a été publiée par l'ANSSI le 10 avril 2013.

Le chiffrement et l'authentification que procurent OpenSSH font que ces outils sont couramment utilisés pour l'administration à distance, le transfert de fichiers, les redirections et encapsulations de flux sensibles sécurisés.

Il est toutefois essentiel de maîtriser la configuration d'OpenSSH, de durcir son installation et d'appliquer des règles d'hygiène strictes pour pouvoir profiter de la sécurité que peuvent apporter ces outils.

Le CERTA recommande aux intégrateurs et adminstrateurs sytèmes et réseaux la lecture et l'application des recommandations de cette note technique pour installer et administrer au mieux un parc avec le protocole SSH et son implémentation de référence : OpenSSH.

Documentation

- Recommandations pour un usage sécurisé d'(Open)SSH :
  http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-des-reseaux/recommandations-pour-un-usage-securise-d-open-ssh.html

5 Rappel des avis émis

Dans la période du 12 au 18 avril 2013, le CERTA a émis les publications suivantes :

- CERTA-2013-AVI-244 : Multiples vulnérabilités dans les systèmes SCADA Schneider
- CERTA-2013-AVI-245 : Vulnérabilité dans Xen qemu-nbd
- CERTA-2013-AVI-246 : Multiples vulnérabilités dans Oracle Database Server
- CERTA-2013-AVI-247 : Multiples vulnérabilités dans Oracle Fusion Middleware
- CERTA-2013-AVI-248 : Multiples vulnérabilités dans Oracle Applications
- CERTA-2013-AVI-249 : Multiples vulnérabilités dans Oracle Industry Applications
- CERTA-2013-AVI-250 : Multiples vulnérabilités dans Oracle Financial Services Software
- CERTA-2013-AVI-251 : Multiples vulnérabilités dans Oracle Primavera Products Suite
- CERTA-2013-AVI-252 : Multiples vulnérabilités dans Oracle Solaris
- CERTA-2013-AVI-253 : Multiples vulnérabilités dans Oracle MySQL
- CERTA-2013-AVI-254 : Multiples vulnérabilités dans Oracle GlassFish Server
- CERTA-2013-AVI-255 : Vulnérabilité dans Oracle Support Tools
- CERTA-2013-AVI-256 : Multiples vulnérabilités dans Oracle Java
- CERTA-2013-AVI-257 : Multiples vulnérabilités dans Apple OS X
- CERTA-2013-AVI-258 : Vulnérabilité dans Apple Safari
- CERTA-2013-AVI-259 : Multiples vulnérabilités dans le noyau Linux de Red Hat
- CERTA-2013-AVI-260 : Vulnérabilité dans Cisco NAC Manager
- CERTA-2013-AVI-261 : Vulnérabilité dans Cisco TelePresence Infrastructure

Gestion détaillée du document

19 avril 2013 version initiale.