Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 21 juin 2013
N° CERTA-2013-ACT-025

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2013-ACT-025

1 Correctifs Oracle Java

Dans le cadre de son cycle de diffusion des mises à jour, Oracle a publié une nouvelle version de Java JRE et JDK.

Cette mise à jour corrige quarante vulnérabilités critiques. Ces dernières concernent différents sous-composants de Java tels que la gestion des graphiques, du son, de la sérialisation, etc. La plupart de ces vulnérabilités permettent l'exécution de code arbitraire à distance ainsi qu'une atteinte à la confidentialité ou l'intégrité des données.

Le CERTA recommande d'appliquer cette mise à jour le plus rapidement possible lorsque la désactivation de Java dans le navigateur n'est pas envisageable, et de suivre les règles de base de sécurité suivantes :

- prendre garde aux liens transmis par courriels ;
- faire preuve de vigilance lors de la consultation de sites Web non vérifiés.

Documentation

- Bulletin de sécurité Oracle JavaCPUJun2013 du 18 juin 2013 :
  http://www.oracle.com/technetwork/topics/security/javacpujun2013-1899847.html
- Bulletin d'actualité du CERTA sur la publication par Microsoft d'un « Fix it » pour désactiver Java dans Internet Explorer :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-ACT-024/

2 Vulnérabilité dans Puppet

Le CERTA a publié un avis concernant une vulnérabilité corrigée dans le logiciel de gestion de configuration Puppet.

L'exploitation de cette vulnérabilité, due à un manque de vérification des données envoyées au serveur, peut avoir des conséquences très importantes, allant de l'exécution de code sur le serveur Puppet, à la prise de contrôle de l'ensemble des machines administrées via ce logiciel. Des codes malveillants exploitant cette faille ont commencé à circuler sur Internet quelques heures après la publication du correctif de sécurité.

Le CERTA recommande aux utilisateurs de ce logiciel de déployer la mise à jour le plus rapidement possible et de s'assurer qu'aucune activité malveillante n'a eu lieu sur le serveur pendant la période où celui-ci était vulnérable (en vérifiant l'intégrité des fichiers de configuration et en analysant les journaux du serveur pour valider l'absence d'activité suspecte).

Il est également rappelé qu'une séparation physique ou logique du réseau d'administration, comme préconisée dans le guide d'hygiène de l'ANSSI, est fortement conseillée et permet de limiter la surface d'attaque d'un système d'information confronté à des vulnérabilités de ce type.

Documentation

- Avis CERTA-2013-AVI-368 du 20 juin 2013 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-368/
- Guide d'hygiène informatique :
  http://www.ssi.gouv.fr/IMG/pdf/guide_hygiene_informatique_anssi.pdf

3 Sortie de la version stable de EMET 4.0

Le 18 juin 2013 *Microsoft* a publié la version finale 4.0 de l'outil EMET (Enhanced Mitigation Experience Toolkit). Cette nouvelle version n'apporte pas de fonctionnalités supplémentaires par rapport à la version 4.0 béta dont les caractéristiques principales ont été présentées dans le bulletin CERTA-2013-ACT-017. À noter, cette version est la première publiée par *Microsoft* depuis son annonce d'assurer un support pour l'utilisation professionnelle de ce produit.

Le CERTA recommande l'intégration de cet utilitaire dans les systèmes d'information dès que possible. Il reste cependant pertinent de qualifier cette intégration avant tout déploiement d'ampleur, afin d'éviter d'éventuels effets de bord sur les applications métier.

Documentation

- Bulletin de publication d'EMET par Microsoft :
  http://blogs.technet.com/b/srd/archive/2013/06/17/emet-4-0-now-available-for-download.aspx
- Page de téléchargement de EMET 4.0 :
  http://www.microsoft.com/en-us/download/details.aspx?id=39273
- Bulletin d'actualité CERTA-2012-ACT-016 du 20 avril 2012 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-ACT-016/
- Bulletin d'actualité CERTA-2013-ACT-017 du 26 avril 2013 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-ACT-017/

4 Rappel des avis émis

Dans la période du 14 au 20 juin 2013, le CERTA a émis les publications suivantes :

- CERTA-2013-AVI-356 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu
- CERTA-2013-AVI-357 : Multiples vulnérabilités dans IBM Notes
- CERTA-2013-AVI-358 : Vulnérabilité dans Parallels Plesk Panel
- CERTA-2013-AVI-359 : Multiples vulnérabilités dans Novell ZENworks
- CERTA-2013-AVI-360 : Multiples vulnérabilités dans Siemens WinCC Web Navigator
- CERTA-2013-AVI-361 : Multiples vulnérabilités dans Oracle Java
- CERTA-2013-AVI-362 : Multiples vulnérabilités dans Oracle Solaris
- CERTA-2013-AVI-363 : Multiples vulnérabilités dans Apple OS X
- CERTA-2013-AVI-364 : Vulnérabilité dans Google Chrome
- CERTA-2013-AVI-365 : Vulnérabilité dans FreeBSD
- CERTA-2013-AVI-366 : Multiples vulnérabilités dans Cisco TelePresence
- CERTA-2013-AVI-367 : Multiples vulnérabilités dans EMC RSA BSAFE
- CERTA-2013-AVI-368 : Vulnérabilité dans Puppet

Gestion détaillée du document

21 juin 2013 version initiale.