Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 18 janvier 2013
N° CERTA-2013-ACT-003

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2013-ACT-003

1 Vulnérabilités dans Oracle Java

Cette semaine, Oracle a publié la version 7 mise à jour 11 de la JRE et la JDK de Java. Cette mise à jour, qui intervient en dehors du cycle de mise à jour d'Oracle, corrige la vulnérabilité portant la référence CVE-2013-0422 objet de l'alerte CERTA-2013-ALE-001.

Un code ciblant cette faille est largement utilisé dans des kits d'exploitation depuis plusieurs mois. Ces derniers jours, la divulgation publique de ce code d'exploitation a entrainé une augmentation grandissante du nombre d'attaques.

Le code d'exploitation profite de deux vulnérabilités pour désactiver le gestionnaire de sécurité (*Security Manager*).

- La première vulnérabilité permet d'utiliser la méthode « findClass » de la classe MBeanInstantiator. Elle permet de charger une classe dans l'espace de noms (*namespace*) système ;
- La deuxième vulnérabilité concerne la nouvelle API « Reflection » de Oracle Java. Cette API est disponible à partir de la version 1.7 du produit. La vulnérabilité découle d'un défaut de vérification lors d'un appel de méthode via l'API « Reflection ». Cette vulnérabilité est utilisée pour appeler des méthodes des classes qui ont été chargées via la première vulnérabilité.

L'association des deux vulnérabilités permet au code d'exploitation de définir une classe arbitraire avec les droits système, qui va désactiver le gestionnaire de sécurité de l'*applet* Java pour exécuter du code arbitraire à distance.

La mise à jour d'Oracle corrige la deuxième vulnérabilité. Il est toujours possible d'utiliser la première vulnérabilité dans un *applet* pour charger des classes dans l'espace de noms système. Cependant des vérifications ont été rajoutées dans l'API « Reflection ». Il n'est donc plus possible d'utiliser la deuxième vulnérabilité pour appeler des méthodes sur les classes dans l'espace de noms système.

La mise à jour Java 1.7.11 a augmenté le niveau de sécurité des *applets* Java et des applications Web de « moyen » à « haut ». L'utilisateur est averti lorsque un *applet* non signé est chargé dans le navigateur. Cela permet d'empêcher l'exécution automatique et silencieuse d'un *applet* Java sur le poste client.

Le CERTA recommande d'appliquer la mise à jour le plus rapidement possible et de suivre les règles de base de sécurité qui sont :

- de prendre garde aux liens qui sont dans les courriels ;
- de faire preuve de vigilance lorsque vous consultez des sites Web non vérifiés.

Documentation

- Vulnérabilité dans Oracle Java :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-ALE-001/index.html
- Bulletin de version Oracle :
  http://www.oracle.com/technetwork/java/javase/7u11-relnotes-1896856.html
- Bulletin d'alerte Oracle CVE-2013-0422 :
  http://www.oracle.com/technetwork/topics/security/alert-cve-2013-0422-1896849.html

2 Caractéristiques et limitations de EMET de Microsoft

Enhanced Mitigation Experience Toolkit (EMET) est un outil développé par *Microsoft* permettant la réduction de risques liés aux failles applicatives. Pour l'utiliser, il faut déterminer les processus à protéger ainsi que les protections à apporter pour chacun d'entre eux. Le CERTA conseille régulièrement l'intégration dans les systèmes d'informations, car de nombreuses attaques peuvent être bloquées par ce produit. Plusieurs des options de sécurité d'EMET ont déjà été évoquées dans le bulletin CERTA-2012-ACT-016 (cf Documentation).

Les administrateurs cherchent souvent à intégrer EMET lors de la publication d'une vulnérabilité dite *0day*, mais ce processus devrait être anticipé dans le cadre d'une défense en profondeur et non en réponse à une menace directe. En effet, si l'utilisation d'EMET est vivement souhaitable, il ne faut pas minimiser son déploiement, car comme pour tout déploiement, de nombreux tests de non régression doivent être effectués. De plus, EMET ne saura pas toujours bloquer l'exploitation de certaines failles, comme c'était par exemple le cas dans la dernière vulnérabilité *Java* (CERTA-2013-ALE-001). EMET ne saurait donc être considéré comme une protection absolue, mais comme l'une des composantes souhaitables de la défense en profondeur du système d'information, afin d'en réduire la surface d'attaque.

Deux versions de EMET peuvent être utilisées, la 3.0 et la 3.5. La version 3.0 est la dernière version stable et la version 3.5 est encore en test, mais propose de nombreuses protections supplémentaires. Le CERTA recommande donc d'envisager l'utilisation de la version 3.5 en priorité et, si les contraintes sont trop fortes, de basculer sur la version 3.0. Dans les deux cas, les applications protégées seront moins sensibles aux attaques courantes. À noter que EMET, comme la majorité des produits de *Microsoft*, est maintenu par l'éditeur.

Documentation

- Bulletin d'actualité CERTA-2012-ACT-016 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-ACT-016
- Bulletin d'alerte CERTA-2012-ALE-001 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-ALE-001
- Présentation de EMET 3.5 :
  http://blogs.technet.com/b/srd/archive/2012/07/24/emet-3-5-tech-preview-leverages-security-mitigations-from-the-bluehat-prize.aspx
- Téléchargement de EMET 3.5 :
  http://www.microsoft.com/en-us/download/details.aspx?id=30424
- Téléchargement de EMET version 3.0 :
  http://www.microsoft.com/en-us/download/details.aspx?id=29851

3 Correctif d'une vulnérabilité Internet Explorer

Fin décembre 2012, le CERTA diffusait l'alerte CERTA-2012-ALE-010 sur une vulnérabilité critique affectant les versions 6, 7 et 8 de Microsoft Internet Explorer. Cette vulnérabilité, largement diffusée et activement exploitée, permet l'exécution de code à distance au moyen d'une page Web spécialement conçue.

Après avoir diffusé un correctif provisoire fin décembre, Microsoft a publié cette semaine une mise à jour hors cycle pour les systèmes impactés (MS13-008).

Le CERTA recommande vivement l'application de cette mise à jour dans les meilleurs délais.

Documentation

- Alerte CERTA-2012-ALE-010 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-ALE-010
- Bulletin de sécurité Microsoft MS13-008 du 14 janvier 2013 :
  http://technet.microsoft.com/fr-fr/security/bulletin/MS13-008
  http://technet.microsoft.com/en-us/security/bulletin/MS13-008
- Bulletin d'actualité CERTA-2013-ACT-002 « Caractéristiques et limitations des Fix It de Microsoft » :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-ACT-002

4 Correctifs Oracle

Oracle a publié cette semaine des mises à jour corrigeant de nombreuses vulnérabilités dans certains de ses produits tels que MySQL, Oracle Database Mobile/Lite, Virtual Box 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. Notons que la dernière vulnérabilité Java (portant la référence « CVE-2013-0422 ») n'est pas concernée par le bulletin de sécurité Oracle, celle-ci ayant déjà fait l'objet d'un bulletin hors cycle le 13 Janvier 2013.

Il est important de noter que 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.

4.1 Documentation

- Bulletin de sécurité Oracle du 15 Janvier 2013 :
  http://www.oracle.com/technetwork/topics/security/cpujan2013-1515902.html

5 Rappel des avis émis

Dans la période du 11 au 17 janvier 2013, le CERTA a émis les publications suivantes :

- CERTA-2013-AVI-023 : Multiples vulnérabilités dans Google Chrome
- CERTA-2013-AVI-024 : Vulnérabilités dans Ruby on Rails
- CERTA-2013-AVI-025 : Vulnérabilité dans Citrix CloudPlatform
- CERTA-2013-AVI-026 : Vulnérabilité dans le système SCADA Siemens Simatic RF Manager
- CERTA-2013-AVI-027 : Vulnérabilité dans IBM TS3310 Tape Library
- CERTA-2013-AVI-028 : Multiples vulnérabilités dans Avaya Call Management System
- CERTA-2013-AVI-029 : Multiples vulnérabilités dans Adobe ColdFusion
- CERTA-2013-AVI-030 : Vulnérabilité dans Samba
- CERTA-2013-AVI-031 : Multiples vulnérabilités dans Oracle Sun Products Suite
- CERTA-2013-AVI-032 : Vulnérabilité dans Oracle JD Edwards
- CERTA-2013-AVI-033 : Vulnérabilité dans Oracle Virtualization
- CERTA-2013-AVI-034 : Multiples vulnérabilités dans Oracle MySQL
- CERTA-2013-AVI-035 : Multiples vulnérabilités dans Oracle Siebel CRM
- CERTA-2013-AVI-036 : Vulnérabilité dans Oracle Database Server
- CERTA-2013-AVI-037 : Multiples vulnérabilités dans Oracle E-Business Suite
- CERTA-2013-AVI-038 : Multiples vulnérabilités dans Oracle PeopleSoft Products
- CERTA-2013-AVI-039 : Multiples vulnérabilités dans Oracle Database Mobile/Lite Server
- CERTA-2013-AVI-040 : Multiples vulnérabilités dans Oracle Enterprise Manager Grid Control
- CERTA-2013-AVI-041 : Multiples vulnérabilités dans Oracle Fusion Middleware
- CERTA-2013-AVI-042 : Vulnérabilité dans Oracle Supply Chain Products Suite
- CERTA-2013-AVI-043 : Vulnérabilité dans IBM Cognos TM1
- CERTA-2013-AVI-044 : Vulnérabilité dans Cisco ASA 1000V Cloud Firewall H323

– CERTA-2013-AVI-045 : Multiples vulnérabilités dans Xen
– CERTA-2013-AVI-046 : Multiples vulnérabilités dans Drupal
– CERTA-2013-AVI-047 : Multiples vulnérabilités dans le système SCADA Rockwell Automation Controllogix

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

– CERTA-2012-ALE-010-003 : Vulnérabilité dans Internet Explorer (fermeture de l'alerte, suite à la diffusion du correctif par l'éditeur)
– CERTA-2012-INF-001-001 : Dénis de service - Prévention et réaction (modifications mineures)
– CERTA-2013-ALE-001-002 : Vulnérabilités dans Oracle Java (mise à jour systèmes affectés)

Gestion détaillée du document

18 janvier 2013 version initiale.