Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 14 décembre 2012
N° CERTA-2012-ACT-050

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2012-ACT-050

1 Alerte pour Oracle MySQL

Le 06 décembre 2012, le CERTA a publié une alerte pour *Oracle MySQL*. Cette alerte intervient après la publication le 1er décembre 2012 d'une preuve de concept sur une liste non restreinte de sécurité. Cette preuve de concept montre qu'il est possible de provoquer un débordement de mémoire tampon dans la pile et de contrôler le flux d'exécution pour executer du code malveillant. L'attaque nécessite un compte sur le serveur MySQL. Les hébergeurs mutualisés sont donc particulièrement exposés car il est possible d'exécuter du code arbitraire avec les droits du processus « mysqld ».

Cette vulnérabilité porte la référence CVE-2012-5611 et concerne toutes les versions de *Oracle MySQL*. Contrairement à certaines informations relayées, cette vulnérabilité est aussi présente sur la plate-forme Microsoft Windows. La complexité de l'exploitation de cette vulnérabilité sur Microsoft Windows XP ou Microsoft Windows Server 2003 est faible.

Le CERTA tient à signaler que la vulnérabilité a été corrigée pour *MariaDB* le 29 novembre 2012 (voir CERTA-2012-AVI-701 et bulletin de sécurité MariaDB 5528a). *MariaDB* est une version de MySQL sous licence GPL et maintenue par la communauté du libre. *MariaDB* n'était donc plus vulnérable au moment de la divulgation de la preuve de concept.

Dans l'attente d'un correctif de l'éditeur Oracle, le CERTA recommande de se référer aux facteurs atténuants de l'alerte CERTA-2012-ALE-007.

Documentation

- Alerte CERTA-2012-ALE-007 - Vulnérabilité dans MySQL :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-ALE-007/index.html
- Avis CERTA-2012-AVI-701 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-701/
- Référence CVE-2012-5611 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5611
  http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-5611
- MySQL (Linux) Stack Based buffer overrun PoC Zeroday :
  http://seclists.org/fulldisclosure/2012/Dec/4

2 Correctifs de la semaine

Cette semaine de nombreux correctifs de sécurités ont été diffusés.
Microsoft a publié ses correctifs de sécurité mensuels, cinq d'entre eux sont estimés comme « critiques » par l'éditeur. Ils concernent :

- des vulnérabilités dans *Internet Explorer* (MS12-077) ;
- des vulnérabilités dans les pilotes en mode noyau de Windows (MS12-078) ;
- une vulnérabilité dans *Microsoft Word* (MS12-079) ;
- une vulnérabilité dans *Microsoft Exchange Server* (MS12-080) ;
- une vulnérabilité dans le composant de traitement des fichiers de *Windows* (MS12-081).

Microsoft n'a pas constaté d'exploitation de ces vulnérabilités avant la publication de ses correctifs. Le CERTA attire toutefois l'attention sur la vulnérabilité MS12-081 qui possède une large surface d'attaque.

Adobe a également publié un correctif sur son produit *Flash Player* qui pouvait mener un utilisateur malintentionné à exécuter du code arbitraire à distance. Le CERTA n'a actuellement pas connaissance d'une exploitation de cette vulnérabilité.

Il est important de noter que de nombreuses solutions tiers utilisent les produits évoqués. Des mises à jour de ces solutions sont donc également à surveiller.

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

Documentation

- Synthèse des bulletins de sécurité Microsoft du mois de décembre 2012 :
  http://technet.microsoft.com/fr-fr/security/bulletin/ms12-dec
- Bulletin de sécurité Adobe Flash Player du 11 décembre 2012 :
  http://www.adobe.com/support/security/bulletins/apsb12-27.html

3 Publication par Microsoft d'un guide de mesures permettant de limiter l'impact des vols d'informations d'authentification en environnement Active Directory

Microsoft a publié cette semaine un document dédié aux mesures défensives permettant de limiter l'impact des vols d'informations d'authentification dans un environnement Active Directory.

Lors d'une compromission, un attaquant qui a réussi à obtenir un accès en administrateur local à un poste récupère les informations d'authentification des différents utilisateurs authentifiés sur ce poste (couple identifiant/mot de passe ou condensat du mot de passe). Ces informations d'authentification peuvent être retrouvées en mémoire ou sur le disque. L'attaquant peut ensuite réutiliser ces informations pour se connecter à de nouveaux postes ou serveurs. Il peut alors répéter le processus de récupération des informations d'authentification sur ces postes en cherchant à obtenir des comptes privilégiés. Le CERTA a constaté dans de multiples incidents l'utilisation de ces techniques par les attaquants pour se propager sur les réseaux réussir et obtenir des comptes privilégiés.

Afin de limiter l'impact de ces attaques le document propose trois mesures principales.

La première concerne la protection des comptes privilégiés du domaine. Elle a pour but d'empêcher un attaquant ayant compromis un poste d'utilisateur de pouvoir récupérer les informations d'authentification d'un compte privilégié. Pour cela les actions suivantes sont proposées :

- interdire aux comptes privilégiés du domaine de s'authentifier sur des stations de confiance moindre ;
- fournir aux administrateurs des comptes d'administration distincts de leur compte utilisateur classique ;
- dédier des stations durcies aux tâches d'administration ;
- configurer les services et tâches planifiées pour ne pas utiliser de comptes du domaine privilégiés sur les systèmes exposés comme les postes de travail des utilisateurs.

La seconde mesure porte sur la protection des comptes locaux disposant de privilèges d'administration. L'objectif de cette mesure est d'empêcher la réutilisation sur d'autres machines d'un compte d'administration local compromis. Pour réaliser cela il est recommandé :

– d'interdire l'accès à distance aux comptes d'administration locaux ;
– il est également conseillé de créer des mots de passes uniques pour les comptes d'administration locaux.

Enfin la dernière mesure proposée consiste à restreindre le trafic entre les différentes machines du réseau à l'aide d'un pare-feu local. Le trafic entre machines du réseau ne doit être autorisé que depuis des emplacements identifiés au préalable comme légitimes (assistance informatique, serveur de gestion, ...). Cette mesure a pour objectif d'empêcher un attaquant de réutiliser des informations d'authentification pour compromettre de nouvelles machines.

Des recommandations complémentaires sont également exposées dans ce document, notamment :

– la suppression des utilisateurs standards du groupe Administrateur local ;
– la mise en place de mesures empêchant les comptes privilégiés d'accéder directement à des donnnées en provenance d'Internet: en mettant en place du filtrage au niveau des serveurs mandataires HTTP et en s'assurant que ces comptes n'ont pas de boîte aux lettres électroniques ;
– l'utilisation d'outils d'administration à distance qui ne placent pas d'information de connexions en mémoire sur le poste distant (MMC);
– la mise à jour des applications et du système d'exploitation ;

D'autres attaques de type vol d'informations d'authentification sont également abordées dans le document.
Enfin, ce document donne les procédures permettant de mettre en place, pas à pas, les mesures proposées.

Les mesures présentées dans ce document permettent d'élever le niveau de sécurité d'un parc informatique, le CERTA recommande donc leur application une fois leur impact sur le système d'information qualifié.

Documentation

– Billet du blog *Trustworthy Computing* du 11 décembre 2012 :

  http://blogs.technet.com/b/trustworthycomputing/archive/2012/12/11/mitigating-targeted-attacks-on-your-organization.aspx

4 Rappel des avis émis

Dans la période du 07 au 13 décembre 2012, le CERTA a émis les publications suivantes :

– CERTA-2012-AVI-705 : Multiples vulnérabilités dans le système SCADA Schneider Electric Ezylog
– CERTA-2012-AVI-706 : Multiples vulnérabilités dans Apache Tomcat
– CERTA-2012-AVI-707 : Vulnérabilité dans ISC BIND
– CERTA-2012-AVI-708 : Vulnérabilité dans les imprimantes HP LaserJet Pro 400
– CERTA-2012-AVI-709 : Vulnérabilité dans les imprimantes HP Color LaserJet
– CERTA-2012-AVI-710 : Vulnérabilité dans HP Network Node Manager
– CERTA-2012-AVI-711 : Vulnérabilité dans IBM Informix
– CERTA-2012-AVI-712 : Vulnérabilité dans IBM Tivoli Monitoring
– CERTA-2012-AVI-713 : Vulnérabilité dans Avaya Experience Portal
– CERTA-2012-AVI-714 : Multiples vulnérabilités dans IBM Rational
– CERTA-2012-AVI-715 : Vulnérabilité dans IBM Tivoli Directory Server
– CERTA-2012-AVI-716 : Multiples vulnérabilités dans IBM WebSphere Application Server
– CERTA-2012-AVI-717 : Multiples vulnérabilités dans Internet Explorer
– CERTA-2012-AVI-718 : Vulnérabilité dans Microsoft Word
– CERTA-2012-AVI-719 : Multiples vulnérabilités dans Microsoft Exchange Server
– CERTA-2012-AVI-720 : Multiples vulnérabilités dans les pilotes en mode noyau de Windows
– CERTA-2012-AVI-721 : Vulnérabilité dans le composant de traitement des fichiers dans Windows
– CERTA-2012-AVI-722 : Vulnérabilité dans Microsoft Windows DirectPlay
– CERTA-2012-AVI-723 : Vulnérabilité dans le composant Windows IP-HTTPS
– CERTA-2012-AVI-724 : Multiples vulnérabilités dans Google Chrome

- CERTA-2012-AVI-725 : Vulnérabilité dans Adobe ColdFusion
- CERTA-2012-AVI-726 : Multiples vulnérabilités dans Adobe Flash Player
- CERTA-2012-AVI-727 : Vulnérabilités dans HP OpenVMS LOGIN et ACMELOGIN
- CERTA-2012-AVI-728 : Vulnérabilités dans Symantec Endpoint Protection
- CERTA-2012-AVI-729 : Vulnérabilités dans Bluecoat IntelligenceCenter et ProxySG
- CERTA-2012-AVI-730 : Vulnérabilité dans le système SCADA Siemens Automation License Manager
- CERTA-2012-AVI-731 : Vulnérabilité dans IBM SPSS Modeler Premium
- CERTA-2012-AVI-732 : Vulnérabilité dans Citrix XenDesktop
- CERTA-2012-AVI-733 : Vulnérabilité dans Citrix XenApp
- CERTA-2012-AVI-734 : Vulnérabilité dans les produits Avaya

Gestion détaillée du document

14 décembre 2012 version initiale.