Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 17 janvier 2014
N° CERTA-2014-ACT-003

**Affaire suivie par :**
CERTA

# BULLETIN D'ACTUALITÉ

**Objet : Bulletin d'actualité CERTA-2014-ACT-003**

## 1 Détournement du protocole NTP permettant des dénis de service par amplification

Le protocole NTP (*Network Time Protocol*) est utilisé pour la synchronisation des horloges d'équipements informatiques (serveurs, postes de travail, équipements d'infrastructure, etc.) à travers le réseau. Ce protocole est important car le fonctionnement de nombreux services s'appuie sur la notion de temps, indispensable pour permettre la corrélation des actions réalisées au niveau du système d'information.

Récemment, il est apparu qu'une mauvaise configuration du service implémentant le protocole NTP permettait à des attaquants de réaliser des attaques de type déni de service distribué par amplification.

Le principe de ce type d'attaque consiste à usurper l'adresse IP d'une victime et à envoyer une requête à un service tiers (comme déjà vu précédemment avec les services DNS ou CHARGEN) générant une réponse de taille bien plus importante que celle de la requête initiale.

Le protocole NTP repose sur la couche UDP qui est un protocole « non connecté » et ne permet pas de se prémunir contre l'usurpation des adresses IP source. Ainsi un attaquant peut envoyer sur Internet des datagrammes UDP spécialement conçus, ayant pour IP source l'adresse de sa victime, à un serveur NTP mal configuré. Ce dernier enverra par la suite sa réponse à la victime.

En plus de leurs fonctionnalités principales, les serveurs NTP peuvent répondre à des requêtes, normalement réservées aux administrateurs, permettant de connaître en temps réel le trafic engendré par les clients connectés.

Ces courtes requêtes font l'objet de réponses de la part du serveur de taille bien plus importante allant de 3660 à 5500 fois la taille de la requête initiale.

Dans la configuration par défaut du service NTPd ces commandes sont accessibles par défaut. Une mise à jour récente du service permet de bloquer ces dernières. Cependant d'autres implémentations propriétaires peuvent aussi être impactées.

S'il n'est pas possible de mettre à jour ce service, le CERTA recommande de vérifier la configuration de ce dernier afin de s'assurer que les commandes de type « `GETLIST` » ne soient pas accessibles depuis Internet.

### Documentation

- Bulletin de sécurité NTPd :
  http://support.ntp.org/bin/view/Main/SecurityNoticeDRDoS_Amplification_Attack_using
- Avis CERTA-2014-AVI-034 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2014-AVI-034/index.html
- Exemples de configurations pour différentes versions de ntpd :
  http://www.team-cymru.org/ReadingRoom/Templates/secure-ntp-template.html

# 2 Mise en œuvre des mécanismes de sécurité du noyau Linux dans Android

Le système d'exploitation Android est particulièrement novateur en matière de sécurité, parmi les systèmes utilisant le noyau Linux. La version 4.4 (dite « *Kit-Kat* ») du système d'exploitation Android a été publiée en octobre 2013. Elle intègre plusieurs améliorations de sécurité, la plus importante étant la mise en place d'un bac à sable pour les applications. Ce mécanisme d'isolation repose sur `SELinux`, une fonctionnalité présente par défaut dans tous les noyaux Linux 2.6. Le contrôle d'accès discrétionnaire (DAC) classique de Linux est ainsi renforcé par un contrôle d'accès obligatoire (MAC) permettant d'appliquer des politiques de sécurité propres à chaque application. Les conséquences d'une vulnérabilité dans une application pourront de fait être réduites.

Chaque nouvelle version du système Android apporte son lot de fonctionnalités de sécurité, utilisant de nombreuses fonctionnalités offertes par le noyau. On peut citer par exemple, depuis la version 4.3 d'Android, l'utilisation exclusive de capacités (capabilities) stockées dans le système de fichiers pour l'augmentation légitime et temporaire de privilèges : les bits `setuid` et `setgid` ont été enlevés de tous les programmes et seules les capacités nécessaires leur ont été affectées. De plus, les applications installées par l'utilisateur ne peuvent pas rajouter de programmes `setuid`, la partition `/system` étant montée avec l'option `nosuid`.

Ces mécanismes de sécurité limitent les conséquences de l'exploitation réussie d'une vulnérabilité. Afin de rendre plus difficile de telles exploitations, le système Android a été durci :

- la disposition de l'espace d'adressage a été rendue aléatoire (activation de l'ASLR) depuis la version 4.0 ;
- les programmes sont compilés avec l'option PIE de gcc depuis la version 4.1 ;
- les données en mémoire sont protégées contre les modifications malveillantes (drapeau NX) depuis la version 2.3.

D'autre part, plusieurs autres paramètres de durcissement ont été appliqués dès la compilation des programmes du système, notamment pour protéger l'adresse de retour des fonctions (canari utilisé depuis la version 1.5) et pour éviter certains débordements de tampons prévisibles (option « fortify source » de gcc utilisée depuis la version 4.2 sur les bibliothèques du système).

Enfin, plusieurs mécanismes cryptographiques peuvent être mis en place pour protéger les données du système de fichiers. Les données de l'utilisateur peuvent être chiffrées, afin d'éviter qu'elles ne soient lisibles par un attaquant ayant dérobé le périphérique. De plus, le nouveau mécanisme de vérification d'intégrité de périphériques de stockage du noyau Linux (`dm-verity`) est supporté par Android 4.4. Cette fonctionnalité permet de vérifier que le système de fichiers n'a pas été altéré par un programme malveillant en vérifiant au démarrage des empreintes par rapport à une base connue.

Le travail effectué par les développeurs d'Android est remarquable. De très nombreuses fonctionnalités de sécurité récentes du noyau Linux sont utilisées par le système et permettent à Android 4.4 d'être un système très satisfaisant du point de vue de la sécurité. De nombreuses distributions Linux devraient s'inspirer de ces travaux. Par exemple, l'implémentation des capacités par le noyau Linux est complète depuis la version 2.6.24 (datant de 2007). Pourtant, aucune distribution Linux grand public n'a totalement migré vers les capacités, en supprimant complètement les programmes `setuid`.

# 3 Les risques liés à l'envoi d'un rapport d'erreurs

Certains outils logiciels (systèmes d'exploitation, navigateurs Web, etc.) sont configurés pour envoyer automatiquement des rapports d'erreurs à l'éditeur en cas de dysfonctionnement. Ces rapports d'erreurs sont ensuite utilisés afin de constituer une base d'informations pour corriger d'éventuelles erreurs.

Or, le plus souvent, l'utilisateur n'est pas en mesure de maîtriser la teneur des informations transmises via le rapport d'erreur. Il peut contenir des éléments techniques, comme la version du système, du navigateur, ou la marque et le modèle de la machine par exemple. Dans le cas où le composant logiciel défaillant traitait des informations sensibles au moment du plantage, il est possible qu'une partie, voire la totalité de ces informations soit transmise (souvent involontairement) à l'éditeur. La sécurité des protocoles utilisés n'est pas toujours précisée ou configurable. Dès lors, ces informations peuvent être détournées par un attaquant et utilisées pour extraire des informations sensibles, voir faciliter l'exploitation de failles sur la machine à des fins malveillantes.

Si cette fonctionnalité est présente sur des environnements sensibles, le CERTA recommande de la désactiver ou de mettre en place les règles de filtrage permettant de la bloquer. Certains mécanismes offrent la possibilité de centraliser l'ensemble des rapports d'erreurs sur un serveur en interne du système d'information : cette fonctionnalité peut être mise en œuvre afin de mieux qualifier les composants défaillants.

# 4 Mise à jour mensuelle Microsoft

Lors de sa dernière mise à jour mensuelle, Microsoft a publié quatre bulletins de sécurité. Les quatre bulletins suivants sont considérés comme importants :

- MS14-001 qui concerne Microsoft Office, cette mise à jour corrige trois vulnérabilités ;
- MS14-002 qui concerne le noyau Windows, cette mise à jour corrige une vulnérabilité ;
- MS14-003 qui concerne les pilotes en mode noyau de Windows, cette mise à jour corrige une vulnérabilité ;
- MS14-004 qui concerne Microsoft Dynamics AX, cette mise à jour corrige une vulnérabilité.

Les vulnérabilités corrigées dans le correctif MS14-001 pourraient permettre l'exécution de code à distance.

Le correctif MS14-002 corrige la vulnérabilité évoquée dans l'alerte CERTA-2013-ALE-008. Cette mise à jour met donc fin à l'alerte de sécurité.

La vulnérabilité corrigée dans le correctif MS14-003 pourrait permettre une élévation de privilèges.

La vulnérabilité corrigée dans le correctif MS14-004 pourrait permettre un déni de service.

**Documentation**

- Synthèse des bulletins de sécurité Microsoft du mois de janvier 2014 :
  http://technet.microsoft.com/fr-fr/security/bulletin/ms14-jan
- Bulletin d'alerte portant sur une vulnérabilité dans le noyau de Windows :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-ALE-008/
- Avis du CERTA portant sur les bulletins de sécurité de Microsoft :
  - http://www.certa.ssi.gouv.fr/site/CERTA-2014-AVI-014/index.html
  - http://www.certa.ssi.gouv.fr/site/CERTA-2014-AVI-015/index.html
  - http://www.certa.ssi.gouv.fr/site/CERTA-2014-AVI-016/index.html
  - http://www.certa.ssi.gouv.fr/site/CERTA-2014-AVI-017/index.html

# 5 Rappel des avis émis

Dans la période du 10 au 16 janvier 2014, le CERTA a émis les publications suivantes :

- CERTA-2014-AVI-008 : Multiples vulnérabilités dans Avaya Experience Portal
- CERTA-2014-AVI-009 : Multiples vulnérabilités dans Symantec Protection Manager
- CERTA-2014-AVI-010 : Multiples vulnérabilités dans le noyau Linux de Mandriva
- CERTA-2014-AVI-011 : Vulnérabilité dans Cisco Small Business Devices
- CERTA-2014-AVI-012 : Vulnérabilité dans McAfee Vulnerability Manager
- CERTA-2014-AVI-013 : Vulnérabilité dans ISC BIND
- CERTA-2014-AVI-014 : Multiples vulnérabilités dans Microsoft Office
- CERTA-2014-AVI-015 : Vulnérabilité dans le noyau Microsoft
- CERTA-2014-AVI-016 : Vulnérabilité dans les pilotes en mode noyau de Microsoft
- CERTA-2014-AVI-017 : Vulnérabilité dans Microsoft Dynamics AX
- CERTA-2014-AVI-018 : Multiples vulnérabilités dans Adobe Reader
- CERTA-2014-AVI-019 : Multiples vulnérabilités dans Adobe Flash Player
- CERTA-2014-AVI-020 : Multiples vulnérabilités dans Google Chrome
- CERTA-2014-AVI-021 : Multiples vulnérabilités dans Oracle Database Server
- CERTA-2014-AVI-022 : Multiples vulnérabilités dans Oracle Fusion Middleware
- CERTA-2014-AVI-023 : Multiples vulnérabilités dans Oracle Hyperion
- CERTA-2014-AVI-024 : Multiples vulnérabilités dans Oracle E-Business Suite
- CERTA-2014-AVI-025 : Multiples vulnérabilités dans Oracle Supply Chain Products Suite
- CERTA-2014-AVI-026 : Multiples vulnérabilités dans Oracle People Soft Products
- CERTA-2014-AVI-027 : Multiples vulnérabilités dans Oracle Siebel CRM
- CERTA-2014-AVI-028 : Vulnérabilité dans Oracle iLearning
- CERTA-2014-AVI-029 : Vulnérabilité dans Oracle Financial Services Software
- CERTA-2014-AVI-030 : Multiples vulnérabilités dans Oracle Java SE

– CERTA-2014-AVI-031 : Multiples vulnérabilités dans Sun Systems Products Suite
– CERTA-2014-AVI-032 : Multiples vulnérabilités dans Oracle VirtualBox et Apache Tomcat
– CERTA-2014-AVI-033 : Multiples vulnérabilités dans Oracle MySql
– CERTA-2014-AVI-034 : Vulnérabilité dans ntpd
– CERTA-2014-AVI-035 : Multiples vulnérabilités dans Cisco Secure Access Control System

Durant la même période, les publications suivantes ont été mises à jour :
– CERTA-2013-ALE-008-001 : Vulnérabilité critique dans le noyau de Microsoft Windows (fermeture de l'alerte, suite à la diffusion du correctif par l'éditeur.)
– CERTA-2014-AVI-005-001 : Vulnérabilité dans X.Org libXfont (ajout du bulletin de sécurité Red Hat.)

# Gestion détaillée du document

**17 janvier 2014** version initiale.