Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 09 août 2013
N° CERTA-2013-ACT-032

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2013-ACT-032

Conditions d'utilisation de ce document :	`http://www.certa.ssi.gouv.fr/certa/apropos.html`
Dernière version de ce document :	`http://www.certa.ssi.gouv.fr/site/CERTA-2013-ACT-032`

1 Mise à jour Mozilla

Lors de la mise à jour du 6 août 2013 de Mozilla, 13 bulletins de sécurité ont été publiés.

Quatre de ces bulletins sont considérés comme critiques :

- MFSA 2013-63 impactant surtout Mozilla Firefox, corrige deux vulnérabilités (CVE-2013-1701 et CVE-2013-1702) ;
- MFSA 2013-64 impactant surtout Mozilla Firefox, corrige une vulnérabilité (CVE-2013-1704) ;
- MFSA 2013-65 impactant surtout Mozilla Firefox, corrige une vulnérabilité (CVE-2013-1705) ;
- MFSA 2013-69 impactant surtout Mozilla Firefox, corrige une vulnérabilité (CVE-2013-1710).

Toutes ces vulnérabilités peuvent mener un attaquant à exécuter du code arbitraire à distance.

Septs bulletins sont considérés comme importants (MFSA-2013-66, MFSA-2013-68, MFSA-2013-71, MFSA-2013-72, MFSA-2013-73, MFSA-2013-74 et MFSA-2013-75), certaines vulnérabilités permettent à un attaquant de provoquer une atteinte à la confidentialité des données.

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

Documentation

- Avis du CERTA-2013-AVI-463 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-463/index.html

2 Publicité malveillante

La société OpenX, leader dans la diffusion de contenu publicitaire sur internet, a été victime d'une modification du code source de sa régie à son insu.

La version gratuite 2.8.10 de sa gamme de produit, a été compromise par l'insertion d'une porte dérobée en PHP depuis novembre 2012.

Un utilisateur malveillant peut ainsi compromettre le site hébergeant la publicité, en y injectant des commandes malveillantes à distance.

Le fichier incriminé par cette modification subreptice est le fichier d'extension javascript « flowplayer-3.1.1.min.js ».

Le CERTA recommande aux webmestres utilisant cette régie publicitaire de vérifier la version installée. Dans la mesure, où la version installée serait la 2.8.10, il est conseillé à minima de mettre à jour avec le paquetage 2.8.11 qui corrige la vulnérabilité ou idéalement de réinstaller l'ensemble du système ayant hébergé la version compromise.

Documentation

- Dernière mise à jour connue d'OpenX :
  http://download.openx.org/openx-2.8.11.zip
- Blog d'OpenX :
  http://blog.openx.org/08/important-update-for-openx-source-2-8-10-users/
- Informations techniques détaillant l'infection :
  http://forum.openx.org/index.php?showtopic=503521628

3 Vulnérabilité vis-à-vis de canaux auxiliaires dans la librairie GnuPG

3.1 Détails sur la vulnérabilité

Une alerte de sécurité a récemment été levée concernant le logiciel GnuPG. Cette alerte concerne une attaque sur l'algorithme RSA implanté dans la bibliothèque libgcrypt de GnuPG, et a été à l'origine découverte et de sa publication par des chercheurs en cryptologie de l'université d'Adelaide.

L'attaque menée par les chercheurs peut être classée dans la catégorie des attaques par canaux auxiliaires, en ce sens qu'un processus espion est capable d'extraire un secret (par exemple une clé privée) d'un autre processus à cause d'une fuite d'information en général liée au matériel. Cela est normalement impossible du fait du cloisonnement des OS : les protections de la mémoire imposées par le noyau isolent les processus et les empêchent de voler de l'information.

L'élément par lequel la fuite d'information est opérée est la mémoire cache des CPU : c'est une ressource partagée entre tous les processus d'une même machine, et une implantation « naïve » d'algorithmes cryptographiques y fuit éventuellement de l'information. Les attaques utilisant le cache comme canal auxiliaire ne sont pas nouvelles, et plusieurs algorithmes dont AES, DES et RSA ont déjà été attaqués selon ce procédé par le passé. Néanmoins, ces attaques utilisaient pour la plupart le cache L1 (cache de niveau 1 au plus proche du CPU) et nécessitaient beaucoup de mesures pour être efficaces, du fait notamment du fort « bruit » des mesures dans ce cache. Elles supposaient aussi que le processus espion s'exécute sur le même coeur de CPU que le processus espionné.

C'est l'algorithme RSA de GnuPG, implanté sur processeur x86, qui a été en pratique attaqué par les chercheurs. L'innovation de l'attaque réside dans le fait qu'elle exploite le cache L3 le plus éloigné du CPU. Ce cache a l'avantage d'être partagé entre tous les coeurs d'un même CPU Intel, et permet donc au processus espion d'observer depuis un coeur tout ce qu'il se passe sur les autres coeurs. Cela rend l'attaque extrêmement efficace et fournit un espion ayant une résolution temporelle très élevée et des mesures peu bruitées : une clé privée RSA peut être extraite en quelques millisecondes. L'attaque tire principalement son efficacité de deux éléments :

- les bibiliothèques partagées des processus partagent les mêmes pages en mémoire physique;
- l'existence de l'instruction Intel x86 *clflush* permettant de « flusher » sélectivement des lignes de cache de tous les niveaux.

Le processus espion réussit à détecter via *clflush* les diverses phases de l'algorithme d'exponentiation modulaire du RSA, dites *Square and Multiply*. Or l'ordre d'exécution de ces phases est lié aux bits de la clé privée RSA utilisée pour l'exponentiation : trouver cet ordre d'exécution revient à révéler la clé.

3.2 Plateformes présentant un risque

Les plateformes à risque sont celles équipées de CPU x86 récents (Pentium 4 et au delà), tous OS confondus. L'article affirme aussi que l'attaque permet de s'abstraire des barrières de la virtualisation : un processus espion s'exécutant dans une machine virtuelle donnée pourrait extraire la clé d'un processus chiffrant s'exécutant sur l'hôte ou sur une autre machine virtuelle.

Il convient néanmoins de nuancer cette affirmation. L'attaque décrite utilise l'hypothèse forte que les pages de code de la bibiliothèque attaquée (libgcrypt en l'occurrence) sont partagées en mémoire physique. Cette hypothèse est vraie au sein d'un OS, mais ne l'est pas forcément entre machines virtuelles. Seul l'hyperviseur VMWare ESX semble effectuer un tel partage de pages mémoire entre instances de VM et hôte : le succès de cette attaque, lorsqu'il s'agit de virtualisation, se limiterait donc à cet hyperviseur.

3.3 Détails du correctif

Le correctif réalisé par les développeurs de GnuPG consiste à utiliser la contremesure classique *Square and Multiply always* pour l'exponentiation modulaire. Afin de limiter l'impact de ce correctif sur les performances, le

Multiply always n'est appliqué que sur les exposants de type privé (les exposants de type public, non sensibles, restent traités sans incidence avec l'algorithme susceptible d'être attaqué). Le CERTA recommande d'appliquer la mise à jour vers la version 1.4.14 dès que possible.

3.4 Documentation

- Slackware alert SSA:2013-215-01 (gnupg) :
  https://lwn.net/Articles/562187/
- The GNU Privacy Guard :
  http://www.gnupg.org/
- Yuval Yarom and Katrina Falkner. Flush+Reload: a High Resolution, Low Noise, L3 Cache Side-Channel Attack In *Cryptology ePrint Archive, Report 2013/448* :
  http://eprint.iacr.org/2013/448
- GnuPG 1.4.14 :
  http://lists.gnupg.org/pipermail/gnupg-announce/2013q3/000330.html
- Attaque par canal auxiliaire :
  http://fr.wikipedia.org/wiki/Attaque_par_canal_auxiliaire

4 Rappel des avis émis

Dans la période du 02 au 08 août 2013, le CERTA a émis les publications suivantes :

- CERTA-2013-AVI-458 : Vulnérabilité dans Cisco OSPF
- CERTA-2013-AVI-459 : Vulnérabilité dans de multiples produits HP LaserJet
- CERTA-2013-AVI-460 : Vulnérabilité dans Joomla!
- CERTA-2013-AVI-461 : Multiples vulnérabilités dans Symantec Backup Exec
- CERTA-2013-AVI-462 : Vulnérabilité dans le système SCADA MOXA OnCell Gateway
- CERTA-2013-AVI-463 : Multiples vulnérabilités dans des produits Mozilla
- CERTA-2013-AVI-464 : Vulnérabilité dans les systèmes SCADA Schneider
- CERTA-2013-AVI-465 : Vulnérabilité dans Cisco TelePresence

Gestion détaillée du document

09 août 2013 version initiale.