Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 01 mars 2013
N° CERTA-2013-ACT-009

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2013-ACT-009

1 Vulnérabilités dans le noyau Linux

Deux vulnérabilités ont été dévoilées récemment dans le noyau Linux (cf. CERTA-2013-AVI-155). Elles permettent à un utilisateur malveillant d'exécuter du code arbitraire avec les privilèges du noyau et donc de réaliser des élévations de privilèges.

La première vulnérabilité (CVE-2013-0871) est due à une situation de compétition (*race condition*) dans l'appel système `ptrace`. Cet emplacement est particulièrement problématique car cet appel système est accessible sur la quasi totalité des distributions sans restriction. Cependant, l'exploitation semble relativement difficile et aucun code d'exploitation public fiable n'est disponible.

La deuxième vulnérabilité (CVE-2013-1763) concerne la gestion des *sockets* Netlink et a été introduite dans la version 3.3 du noyau. La plupart des distributions serveur ne sont donc pas affectées. Cependant, les utilisateurs de noyaux vulnérables auraient pu être exposés depuis plusieurs mois. En effet, un code d'exploitation a été publié en réaction à la correction de la vulnérablilité et annoncé comme utilisé depuis plusieurs mois.

Le CERTA recommande donc l'application des mises à jour dès que possible (cf. Documentation).

Documentation

– Avis CERTA-2013-AVI-155 :
http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-155/

2 Vulnérabilité *Lucky13*

Deux chercheurs britanniques ont annoncé le 6 février dernier avoir découvert une nouvelle vulnérabilité (appelée *Lucky Thirteen*) contre le protocole de communication sécurisé SSL/TLS.

Le protocole SSL/TLS est sans aucun doute le protocole le plus utilisé pour protéger les communications sur Internet (commerce électronique, banque en ligne...). Issu à l'origine d'une initiative industrielle de Netscape, son développement a été depuis repris par l'IETF, organisme de standardisation de protocoles Internet. Depuis quelques années, ses implémentations font l'objet d'attaques plus ou moins pratiques, mais toujours très médiatisées du fait du rôle central que joue le protocole dans la sécurisation de l'Internet.

L'attaque *Lucky Thirteen* s'incrit dans une lignée d'attaques mises au jour par Vaudenay en 2002. L'objectif de l'attaque est d'obtenir le déchiffrement d'une information chiffrée recueillie par écoute d'une communication protégée. Pour ce faire, l'attaquant perturbe une communication protégée par SSL/TLS en espérant que la suite du déroulement de la communication lui donne de l'information sur le clair qu'il cherche à reconstituer.

L'attaque "Lucky Thirteen" utilise une fuite d'information temporelle : lors d'un déchiffrement erroné une valeur du clair particulière entraîne un temps de calculs cryptographiques légèrement plus long.

Ce type d'attaque est difficile à mettre en œuvre du fait que :

- la différence de temps de calcul est très faible : elle n'est perceptible que si l'attaquant est proche de la machine attaquée (sur le même réseau local) ;
- la survenue d'une erreur est fatale au canal de communication TLS : dès qu'une erreur cryptographique est détectée, le canal de communication est réinitialisé. Cette mesure met fin à toute attaque contre l'instance spécifique du canal de communication et les données qu'elle protège.

Les auteurs de *Lucky Thirteen* identifient deux scénarios dans lesquels l'attaque est néanmoins réalisable :

- attaque du protocole DTLS (variante de TLS pour utilisation sur protocole UDP) : comme ce protocole ne lève pas d'erreur fatale en cas de problème, une même session peut-être utilisée pour déchiffrer une donnée entière ;
- attaque multi-sessions : l'attaque cherche à déchiffrer une donnée qui est répétée de manière prévisible dans un grand nombre de communication TLS (mot de passe, cookie, ...). Le nombre de sessions nécessaire pour réaliser l'attaque reste assez élevé (quelques centaines de milliers de sessions).

Par conséquent l'impact pratique de l'attaque *Lucky Thirteen* contre TLS est limité. L'attaque n'est de plus envisageable que du fait d'une mauvaise implémentation de la procédure à suivre en cas de déchiffrement d'un message erroné induisant des fuites d'information temporelle. Les implémentations les plus répandues, dont OpenSSL, corrigent ce problème (voir avis CERTA-2013-AVI-099). Il est donc conseillé de mettre à jour son système d'exploitation (et donc les bibliothèques SSL). Une solution plus pérenne serait d'adopter un mode de chiffrement authentifié, disponible dans la dernière version du protocole, TLSv1.2. Cette solution permettrait d'utiliser un mode où l'intégrité est vérifiée avant de réaliser le déchiffrement, ce qui ferme tout chemin d'attaque. Elle se heurte cependant à une grande inertie dans le déploiement des versions les plus récentes du protocole TLS.

Documentation

- Document de recherche *Lucky Thirteen: Breaking the TLS and DTLS Record Protocols* de N. AlFardan et K.G. Paterson :
  http://www.isg.rhul.ac.uk/tls/TLStiming.pdf
- Document de recherche *Security Flaws Induced by CBC Padding - Applications to SSL, IPSEC, WTLS...* de S. Vaudenay :
  http://www.iacr.org/archive/eurocrypt2002/23320530/cbc02_e02d.pdf
- Avis CERTA-2013-AVI-099 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-099/

3 Exploitation de vulnérabilités visant le lecteur Flash d'Adobe

Au début du mois de février, de multiples vulnérabilités ont été corrigées dans « Adobe Flash Player ». Le 26 février 2013 un nouveau correctif a été publié. Ces vulnérabilités sont considérées comme critiques, car elles permettent l'éxécution de code arbitraire à distance et leur exploitation s'effectue via une page Web ou un document Microsoft Word spécialement conçu.

Découvertes lors de l'analyse d'attaques de type hameçonnage ciblant des entreprises, ces vulnérabilités ont depuis été intégrées dans différentes plates-formes d'exploitation et sont par conséquent largement utilisées.

Les versions vulnérables du lecteur Flash concernent plusieurs systèmes d'exploitation, le CERTA rappelle qu'il est primordial de s'assurer que la version des logiciels tiers installés est bien la dernière disponible sur l'ensemble des composants du système d'information. En ce qui concerne les utilisateurs de Windows 8 la mise à jour du lecteur Flash intégré se fait via les correctifs Microsoft. À ce titre le CERTA recommande donc l'application de ces correctifs dès que possible.

Documentation

- Avis CERTA-2013-AVI-152 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-152/
- Bulletin d'actualité du CERTA-2013-ACT-008 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-ACT-008/

- Bulletin de sécurité Adobe APSB13-04 :
  http://www.adobe.com/support/security/bulletins/apsb13-04.html
- Bulletin de sécurité Adobe APSB13-08 :
  http://www.adobe.com/support/security/bulletins/apsb13-08.html

4 Rappel des avis émis

Dans la période du 22 au 28 février 2013, le CERTA a émis les publications suivantes :

- CERTA-2013-AVI-146 : Multiples vulnérabilités dans les produits VMware
- CERTA-2013-AVI-147 : Multiples vulnérabilités dans Mozilla Thunderbird
- CERTA-2013-AVI-148 : Multiples vulnérabilités dans Google Chrome
- CERTA-2013-AVI-149 : Vulnérabilité dans Drupal
- CERTA-2013-AVI-150 : Vulnérabilité dans Apache Maven
- CERTA-2013-AVI-151 : Multiples vulnérabilités dans Hitachi Cosminexus
- CERTA-2013-AVI-152 : Multiples vulnérabilités dans Adobe Flash Player
- CERTA-2013-AVI-153 : Multiples vulnérabilités dans Apache HTTP Server
- CERTA-2013-AVI-154 : Vulnérabilité dans Cisco Cloud Portal
- CERTA-2013-AVI-155 : Multiples vulnérabilités dans le noyau Linux
- CERTA-2013-AVI-156 : Multiples vulnérabilités dans Microsoft Internet Explorer
- CERTA-2013-AVI-157 : Multiples vulnérabilités dans les produits Cisco
- CERTA-2013-AVI-158 : Multiples vulnérabilités dans Citrix XenServer

Gestion détaillée du document

01 mars 2013 version initiale.