Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 21 décembre 2012
N° CERTA-2012-ACT-051

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2012-ACT-051

1 Vulnérabilités dans des terminaux mobiles Samsung

Cette semaine le CERTA a publié une alerte concernant une vulnérabilité présente dans des terminaux mobiles qui utilisent le composant «Exynos 4» de Samsung. Elle est exposée par le pilote du composant qui donne aux applications l'accès à l'ensemble de l'espace mémoire physique du noyau sans aucune restriction. Il est alors possible pour une application malveillante d'élever ses privilèges sur le système et d'exécuter du code en tant qu'administrateur (*root*). Des applications utilisant cette vulnérabilité sont déjà présentes sur l'Internet.

Cette vulnérabilité est susceptible d'exposer également des terminaux d'autres constructeurs qui utiliseraient ce composant et ce pilote du constructeur Samsung.

En attendant la publication d'un correctif par le constructeur, le CERTA recommande la plus grande vigilance concernant l'installation d'applications non vérifiées sur ces terminaux.

Documentation

– Alerte CERTA-2012-ALE-008 du 18 décembre 2012 :
http://www.certa.ssi.gouv.fr/site/CERTA-2012-ALE-008/

2 Un code malveillant utilise GoogleDocs

Les cas d'utilisation malveillante des réseaux sociaux ou de l'informatique dans le nuage, voire de *webmails*, se multiplient.

Cette année le CERTA a également été amené à traiter plusieurs incidents en relation avec ces services. *Symantec* a récemment publié un article à propos d'un code malveillant dont les connexions aux serveurs de commande et contrôle passaient par *Google Docs*. Un tel détournement a été rendu possible par une fonctionnalité de visualisation de fichier, à laquelle on peut soumettre une URL, sans vérification de sa malveillance. Ce phénomène rend difficile la détection des flux illégitimes :

– les serveurs destinataires ne sont, par essence, pas malveillants ;
– les flux entre le poste infecté et le serveur sont généralement chiffrés.

Ce comportement confirme également que les *botnets* évoluent vers des alternatives plus discrètes qu'IRC, historiquement utilisé comme protocole de communication, et donc plus difficile à bloquer.

Le CERTA recommande donc de faire preuve de vigilance, voire de réserve, à l'égard de l'utilisation des réseaux sociaux, des services de stockage dans le nuage ou de messagerie en ligne, quelle que soit la réputation de

l'hébergeur.

Il est également préconisé de surveiller de tels flux à des heures qui ne correspondent pas une activité classique de bureau.

Documentation

- Symantec - Malware targeting Windows 8 Uses Google Docs
  http://www.symantec.com/connect/blogs/malware-targeting-windows-8-uses-google-docs
- Bulletin d'actualité CERTA-2009-ACT-045 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2009-ACT-045/

3 Vulnérabilité dans les téléviseurs connectés

Aujourd'hui, certains téléviseurs peuvent être connectés à Internet et/ou à un réseau d'entreprise. Ils sont équipés d'un micrologiciel basé sur le système d'exploitation Linux qui leur permet l'accès à de multiples fonctionnalités (visioconférence, lecture de documents, messagerie, réseaux sociaux, navigation web, etc.).

Récemment, une équipe de chercheurs a réussi à prendre le contrôle total d'un téléviseur connecté Samsung en exploitant une vulnérabilité. Aucun code d'exploitation n'est pour le moment disponible publiquement, mais les conséquences de l'exploitation d'une telle vulnérabilité peuvent être importantes, notamment en terme de fuite d'informations :

- accès à la caméra numérique ainsi qu'au microphone dont ils sont équipés ;
- récupération des données stockées sur les périphériques USB connectés ;
- accès à l'historique du téléviseur ;
- installation de logiciels malveillants ;
- récupération de l'identifiant et du mot de passe du micrologiciel ;
- accès aux données stockées dans la mémoire interne du téléviseur ;
- récupération des identifiants des sites Internet/Intranet visités via le téléviseur.

Il n'existe pas à ce jour de correctif pour les téléviseurs présentant cette vulnérabilité. Dans l'attente de la diffusion d'un correctif par le constructeur, le CERTA recommande donc de déconnecter ce type de téléviseur du réseau de l'entreprise et de l'Internet.

En outre, le CERTA recommande, de manière générale, de prêter attention à tous types d'appareils connectés au réseau Internet, en les intégrant dans la politique de sécurité des systèmes d'information. Ces équipements doivent être mis à jour des correctifs de sécurité du constructeur ou de l'éditeur dès leurs parutions.

4 Rappel des avis émis

Dans la période du 14 au 20 décembre 2012, le CERTA a émis les publications suivantes :

- CERTA-2012-ALE-008 : Vulnérabilité dans certains terminaux mobiles Samsung
- CERTA-2012-AVI-735 : Multiples vulnérabilités dans IBM Rational Publishing Engine
- CERTA-2012-AVI-736 : Vulnérabilités dans IBM Lotus Fondations
- CERTA-2012-AVI-737 : Multiples vulnérabilités dans Bluecoat Reporter
- CERTA-2012-AVI-738 : Vulnérabilités dans Adobe Photoshop Camera Raw
- CERTA-2012-AVI-739 : Multiples vulnérabilités dans Avaya Aura System Manager
- CERTA-2012-AVI-740 : Vulnérabilité dans TWiki
- CERTA-2012-AVI-741 : Vulnérabilité dans IBM ClearQuest
- CERTA-2012-AVI-742 : Vulnérabilité dans IBM FB4WKSTNS
- CERTA-2012-AVI-743 : Vulnérabilité dans IBM Lotus Notes
- CERTA-2012-AVI-744 : Vulnérabilité dans VMware View
- CERTA-2012-AVI-745 : Multiples vulnérabilités dans Huawei E585
- CERTA-2012-AVI-746 : Multiples vulnérabilités dans HP-UX
- CERTA-2012-AVI-747 : Vulnérabilité dans Squid

- CERTA-2012-AVI-748 : Vulnérabilités dans RealPlayer
- CERTA-2012-AVI-749 : Vulnérabilité dans Axway SecureTransport
- CERTA-2012-AVI-750 : Vulnérabilités dans IBM InfoSphere BigInsights
- CERTA-2012-AVI-751 : Vulnérabilités dans IBM Tivoli Storage Manager
- CERTA-2012-AVI-752 : Vulnérabilité dans Zend Framework

Gestion détaillée du document

21 décembre 2012 version initiale.