Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 11 juillet 2013
N° CERTA-2013-ACT-028

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2013-ACT-028

1 Nouvelle faille Android

Récemment, un article de Bluebox a été publié sur la sécurité des ordiphones et tablettes Android. Cet article, qui a été largement repris dans la communauté de la SSI, démontre une attaque qui permettrait de modifier le contenu d'une application Android sans que ces changements n'aient d'impact sur la vérification de sa signature.

Cette "faille" est basée sur plusieurs facteurs:

- le format apk utilisé par les applications Android ;
- la différence d'algorithme de sélection des fichiers pour la vérification des signatures et l'exécution des fichiers.

Il est également à noter que, même si elle est obligatoire lors de l'installation d'une application, la signature ne sert qu'à en identifier l'auteur et non l'intégrité de l'application.

Le format apk repose sur l'utilisation d'une archive de type zip. Ce format permet à un utilisateur d'ajouter un fichier avec le même nom et la même arborescence qu'un fichier déjà présent dans l'archive.

Lorsque une application est installée, sa signature est vérifiée par le système. Cependant, seul le contenu du fichier original est pris en compte pour la vérification de la signature. Le fichier dupliqué ne sera donc pas contrôlé. En revanche, lors de l'exécution de l'application, seul le fichier dupliqué sera utilisé.

Cette vulnérabilite permet donc de voir modifiés les fichiers d'une application existante sans que ces changements ne soient détectés lors de l'installation de l'application.

Même si la criticité de cette faille est importante, elle est à mettre en perspective de son vecteur d'exploitation. En effet, pour parvenir à l'utiliser, un attaquant doit mettre en place un des scénarios suivants:

- compromettre les identifiants d'accès à un marché applicatif d'un développeur pour y déposer sa version malveillante ;
- compromettre un marché applicatif pour y déposer sa version malveillante.
- forcer la victime à installer son application modifiée par l'outil en ligne de commande ou pouvoir accéder physiquement au terminal pour le faire.

Le CERTA recommande de ne pas installer d'applications Android manuellement et de n'utiliser que des marchés applicatifs officiels. Lorsque une installation manuelle est obligatoire, il est nécessaire de s'assurer de l'intégrité de l'application avant son installation.

De plus une vérification régulière de l'intégrité des applications déjà déployées est nécessaire.

Pour cela, il existe plusieurs outils permettant de détecter des applications modifiées et/ou malveillantes:

- différents produits de type anti-virus (à installer sur un ordiphone pour détecter les applications installées malveillantes) ;

– l'outil jarsigner disponible avec Oracle Java (à utiliser sur une machine avant l'installation manuelle de l'application) ;
– l'outil BlueBox Security Scanner (à installer sur un ordiphone pour détecter les applications installées et modifiées).

Documentation

– Bluebox Security Scanner :
https://play.google.com/store/apps/details?id=com.bluebox.labs.onerootscanner

2 Vulnérabilités présentes dans les interfaces de gestion intelligente de matériel

De nombreux fabriquants de serveurs fournissent des cartes de gestion du matériel "hors-bande" permettant de prendre la main à distance et d'effectuer diverses actions (arrêt, redémarrage, prise en main « graphique », etc.). Ces cartes sont souvent intégrées à la carte mère du serveur et disposent d'une interface réseau dédiée. On peut ainsi citer les technologies iLO (HP), DRAC (Dell), ILOM (Sun) ou iRMC (Fujitsu). Ces cartes fournissent différentes interfaces d'administration, telles que :

– Web (HTTP / HTTPS) ;
– console (Telnet / SSH) ;
– VNC ;
– IPMI (*Intelligent Platform Management Interface*) ;
– etc.

IPMI est un ensemble de spécifications décrivant des protocoles de communication permettant l'échange de données sur un bus local ou *via* le réseau (généralement sur le port 623/UDP).

Un chercheur en sécurité (Dan Farmer) a récemment mis en lumière de nombreuses vulnérabilités impactant le protocole réseau d'IPMI, parmi lesquelles :

– la présence de comptes et mots de passe par défaut ;
– le contournement de l'authentification ;
– la récupération à distance des condensats de mot de passe ;
– le stockage des mots de passe en clair dans la configuration.

De plus, des vulnérabilités peuvent également être présentes dans des services tiers, comme UPnP. L'exploitation de ces vulnérabilités peut permettre à un attaquant de simuler un accès physique au serveur *via* le KVM intégré.

Des codes d'exploitations de ces vulnérabilités étant déjà disponibles sur Internet, le CERTA recommande une vigileance accrue sur l'accès et la configuration de ces interfaces. Il est ainsi nécessaire :

– de contrôler l'accès à ces interfaces par la mise en place de filtrage réseau ;
– de désactiver les interfaces non utilisées ;
– de modifier la configuration par défaut sur les interfaces en production ;
– etc.

Pour plus d'informations, se référer au guide de remédiation fourni par le chercheur (cf. partie Documentation).

Documentation

– Article du chercheur Dan Farmer:
http://fish2.com/ipmi/
– Guide de remédiations des vulnérabilités :
http://fish2.com/ipmi/bp.pdf
– Article présentant les codes d'exploitation :
https://community.rapid7.com/community/metasploit/blog/2013/07/02/a-penetration-testers-guide-to-ipmi

3 Publication du rapport 2012 de l'observatoire sur la résilience de l'Internet français

L'observatoire de la résilience de l'Internet français publie son second rapport portant sur l'année 2012. Créé conjointement par l'ANSSI et l'Afnic, l'observatoire vise à étudier et améliorer la résilience de l'Internet.

Comme la précédente, cette nouvelle édition du rapport porte sur les protocoles d'infrastructure BGP et DNS. Les indicateurs techniques et leurs définitions ont évolué afin de prendre en compte les commentaires portant sur le premier rapport.

Dans cette édition, le périmètre d'étude sur BGP a été étendu de 4 à 1270 AS. Deux nouveaux indicateurs ont été ajoutés : RPKI et le respect des bonnes pratiques de routage. Pour ce qui est de DNS, un nouvel indicateur d'importance est proposé: l'étude des résolveurs les plus demandeurs.

Ce nouveau rapport ainsi que l'édition précédente sont disponibles en version électronique aux l'adresses suivantes :

- http://www.ssi.gouv.fr/observatoire
- http://www.afnic.fr/fr/l-afnic-en-bref/actualites/actualites-generales/7115/show/l-observatoire-sur-la-resilience-de-l-internet-francais-publie-son-rapport-2012-1.html

4 Mise à jour mensuelle Microsoft

Lors de la mise à jour mensuelle de *Microsoft*, sept bulletins de sécurité ont été publiés.
Six de ces bulletins sont considérés comme critiques :

- MS13-052 qui concerne *Microsoft Framework .net* et *Silverlight*, cette mise à jour corrige sept vulnérabilités ;
- MS13-053 qui concerne le noyau *Microsoft Windows*, cette mise à jour corrige huit vulnérabilités ;
- MS13-054 qui concerne *Microsoft GDI+*, cette mise à jour corrige une vulnérabilité ;
- MS13-055 qui concerne *Microsoft Internet Explorer*, cette mise à jour corrige dix-sept vulnérabilités ;
- MS13-056 qui concerne *Microsoft DirectShow*, cette mise à jour corrige une vulnérabilité ;
- MS13-057 qui concerne *Microsoft Windows Media Format Runtime*, cette mise à jour corrige une vulnérabilité.

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

Le septième bulletin MS13-058 est considéré comme important : il concerne une vulnérabilité dans *Microsoft Windows Defender* dont l'exploitation peut permettre une élévation de privilèges.

Microsoft a connaissance de codes d'exploitation publics pour les vulnérabilités corrigées par les bulletins MS13-052, MS13-053 et MS13-055. Le CERTA recommande donc l'application de ces correctifs dès que possible.

Documentation

- Synthèse des bulletins de sécurité Microsoft du mois de juillet 2013 :
  http://technet.microsoft.com/fr-fr/security/bulletin/ms13-jul
- Publication de Microsoft « Running in the wild, not for so long » :
  http://blogs.technet.com/b/srd/archive/2013/07/10/running-in-the-wild-not-for-so-long.aspx

5 Mise à jour Adobe

Le 09 juillet 2013, Adobe a publié trois correctifs de sécurité, considérés comme critiques :

- APSB13-17 qui concerne *Adobe Flash Player* ;
- APSB13-18 qui concerne *Adobe Shockwave Player* ;
- APSB13-19 qui concerne *Adobe ColdFusion*.

Les vulnérabilités corrigées peuvent mener un attaquant à exécuter du code arbitraire à distance.
Le CERTA recommande l'application de ces correctifs dès que possible.

Documentation

- Synthèse des bulletins de sécurité publiés par Adobe :
  http://www.adobe.com/support/security

6 Rappel des avis émis

Dans la période du 05 au 10 juillet 2013, le CERTA a émis les publications suivantes :

- CERTA-2013-AVI-390 : Multiples vulnérabilités dans Barracuda SSL VPN
- CERTA-2013-AVI-391 : Multiples vulnérabilités dans le noyau Linux de Ubuntu
- CERTA-2013-AVI-392 : Vulnérabilité dans Siemens COMOS
- CERTA-2013-AVI-393 : Multiples vulnérabilités dans Apple OS X
- CERTA-2013-AVI-394 : Vulnérabilité dans Citrix XenServer
- CERTA-2013-AVI-395 : Vulnérabilité dans EMC Replication Manager
- CERTA-2013-AVI-396 : Vulnérabilité dans EMC RSA Authentication Manager
- CERTA-2013-AVI-397 : Vulnérabilité dans QNX Software Development Platform
- CERTA-2013-AVI-398 : Multiples vulnérabilités dans Microsoft Framework net et Silverlight
- CERTA-2013-AVI-399 : Multiples vulnérabilités dans le noyau Microsoft Windows
- CERTA-2013-AVI-400 : Vulnérabilité dans Microsoft GDI+
- CERTA-2013-AVI-401 : Multiples vulnérabilités dans Microsoft Internet Explorer
- CERTA-2013-AVI-402 : Vulnérabilité dans Microsoft DirectShow
- CERTA-2013-AVI-403 : Vulnérabilité dans Microsoft Windows Media Format Runtime
- CERTA-2013-AVI-404 : Vulnérabilité dans Microsoft Windows Defender
- CERTA-2013-AVI-405 : Multiples vulnérabilités dans Adobe Flash Player
- CERTA-2013-AVI-406 : Vulnérabilité dans Adobe Shockwave Player
- CERTA-2013-AVI-407 : Multiples vulnérabilités dans Adobe ColdFusion
- CERTA-2013-AVI-408 : Multiples vulnérabilités dans Google Chrome
- CERTA-2013-AVI-409 : Vulnérabilité dans Squid

Gestion détaillée du document

11 juillet 2013 version initiale.