Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 07 octobre 2011
N° CERTA-2011-ACT-040

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2011-40

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-2011-ACT-040

Gestion du document

Référence	CERTA-2011-ACT-040
Titre	Bulletin d'actualité 2011-40
Date de la première version	07 octobre 2011
Date de la dernière version	–
Source(s)	–
Pièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

Le bulletin d'actualité est disponible dans son intégralité et au format PDF à l'adresse suivante : http://www.certa.ssi.gouv.fr/site/CERTA-2011-ACT-040.pdf
Un extrait du bulletin, ne reprenant que les articles de la semaine, se trouve en HTML à l'adresse suivante : http://www.certa.ssi.gouv.fr/site/CERTA-2011-ACT-040/

1 Vulnérabilité dans Apache HTTP Server avec le mod_proxy

Une vulnérabilité identifiée par le numéro CVE-2011-3368 a été annoncée via un avis de sécurité sur la liste de diffusion de la fondation `Apache`. Cette vulnérabilité affecte certaines configurations utilisant le module *mod_proxy*. Les versions 1.3, 2.0 et supérieures sont toutes vulnérables. Un correctif à appliquer au code source de la version 2.2.21 du serveur HTTP est disponible auprès de l'éditeur, à l'adresse ci-dessous.

Toutefois, il est possible d'identifier et de contourner la vulnérabilité en analysant et modifiant au besoin la configuration d'`Apache`.

Pour ce faire, il est nécessaire d'identifier toutes les règles de réécriture d'adresse réticulaire, vers une page locale ou distante du même type que l'exemple suivant, qui seraient présentes dans la configuration du serveur.

```
RewriteRule (.*)\.jpg        http://images.example.com$1.jpg [P]
ou
ProxyPassMatch (.*)\.jpg     http://images.example.com$1.jpg
```

Un attaquant peut, à l'aide d'une requête spécialement conçue, forcer le serveur `Apache` ainsi configuré à effectuer des requêtes sur le serveur « images.example.com ». Le problème se situe dans la validation des requêtes transmises au serveur `Apache`.

Dans le cas où il n'est pas possible d'appliquer le correctif fourni par l'éditeur pour compiler une version non affectée, il est possible de contourner la vulnérabilité en modifiant la configuration précédente en :

```
RewriteRule /(.*)\.jpg       http://images.example.com$1.jpg [P]
ou
ProxyPassMatch /(.*)\.jpg    http://images.example.com$1.jpg
```

Le caractère « / » supplémentaire empêche le serveur de valider les requêtes déclenchant la vulnérabilité.

Documentation

- Avis de sécurité Apache :
  http://mail-archives.apache.org/mod_mbox/httpd-announce/201110.mbox/<20111005141541.GA7696@redhat.com>
- Correctif à appliquer sur le code source :
  http://www.apache.org/dist/httpd/patches/apply_to_2.2.21/CVE-2011-3368.patch
- Référence CVE CVE-2011-3368 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3368

2 Vulnérabilités dans les téléphones HTC

Une vulnérabilité a été publiée sur l'Internet et concerne plusieurs terminaux HTC fonctionnant sous Android. En effet, suite à une mise à jour récente, une application du constructeur automatiquement installée permet de collecter et de centraliser un grand nombre d'informations personnelles (contacts, dernières positions GPS connues, historique des appels, SMS, logs système, . . .).

La vulnérabilité vient du fait que n'importe quelle autre application installée sur le téléphone, disposant au minimum des droits d'accès à Internet, peut interroger cette application et extraire sans authentification l'ensemble des données collectées et les transmettre à des tiers.

Dans l'attente d'une mise à jour du constructeur, le CERTA recommande de faire preuve de la plus grande prudence lors de l'installation d'applications sur des ordiphones.

3 Rappel des avis émis

- CERTA-2011-AVI-542 : Vulnérabilités dans Barracuda IM Firewall
- CERTA-2011-AVI-543 : Vulnérabilité dans CISCO IOS
- CERTA-2011-AVI-544 : Multiples vulnérabilités dans la fonction NAT de CISCO IOS
- CERTA-2011-AVI-545 : Vulnérabilité dans Cisco Unified Communications Manager
- CERTA-2011-AVI-546 : Vulnérabilités dans Joomla!
- CERTA-2011-AVI-547 : Vulnérabilité dans VMWare
- CERTA-2011-AVI-548 : Vulnérabilité dans Plone et Zope
- CERTA-2011-AVI-549 : Vulnérabilités dans Novell Identity Manager

4 Actions suggérées

4.1 Respecter la politique de sécurité

La Politique de Sécurité des Systèmes d'Information (PSSI) est l'ensemble formalisé dans un document applicable, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection des systèmes d'information de l'organisme. Elle traduit la reconnaissance officielle de l'importance accordée par la direction générale de l'organisme à la sécurité de ses systèmes d'information. D'une manière générale, elle contient une partie relative aux éléments stratégiques de l'organisme (périmètre, contexte, enjeux, orientations stratégiques en matière de SSI, référentiel règlementaire, échelle de sensibilité, besoins de sécurité, menaces) et une partie relative aux règles de sécurité applicables. Elle constitue donc une traduction concrète de la stratégie de sécurité de l'organisme.

Quoique puisse suggérer ce document, la politique de sécurité en vigueur dans votre service doit primer.

Cette section précise néanmoins quelques mesures générales de nature à vous prémunir contre les agressions décrites dans ce document. En effet, la sécurité des systèmes d'information ne repose pas exclusivement sur des outils, mais aussi sur une organisation et des politiques.

4.2 Concevoir une architecture robuste

A la lumière des enseignements tirés de ce qui a été présenté dans les bulletins d'actualité, il convient de vérifier que les applications mises en oeuvre (ou à l'étude) ont une architecture qui résiste aux incidents décrits.

4.3 Appliquer les correctifs de sécurité

Le tableau 2 rappelle les avis du CERTA correspondant aux applications ou codes malveillants relatifs aux ports étudiés dans les sections précédentes.

4.4 Utiliser un pare-feu

L'application des correctifs sur un parc informatique important n'est probablement pas immédiate. Un pare-feu correctement configuré peut retenir certaines attaques informatiques le temps d'appliquer les correctifs. Cependant un pare-feu peut donner une illusion de protection. Cette protection est brisée par la moindre introduction d'un ordinateur nomade dans la partie protégée. On remarque qu'il y a de nombreux paquets rejetés à destination de ports légitimement utilisés par des applications de prise de main à distance. La téléadministration correspond à une demande qui grandit avec la taille du parc à gérer. Les paquets rejetés montrent le risque associé à ce type d'application. Ce risque peut être amoindri par l'usage correct d'un pare-feu.

4.5 Analyser le réseau

De nombreux paquets rejetés étudiés correspondent aux ports ouverts par divers virus/vers/chevaux de Troie. Si votre politique de sécurité autorise le balayage des ports ouverts sur les postes de travail ou les serveurs, il peut s'avérer utile de le faire régulièrement afin de découvrir les machines potentiellement contaminées avant qu'un intrus ne le fasse à votre place.

L'analyse des journaux de votre pare-feu est une source pertinente d'informations pour la sécurité de votre réseau et de vos systèmes. Cela peut vous aider à anticiper des incidents en remarquant par exemple des activités anormales. Le CERTA peut vous aider dans ce travail d'analyse.

4.6 Réagir aux incidents de sécurité

Organisez-vous pour réagir aux incidents de sécurité, en particulier, pour assurer une certaine continuité dans les équipes d'administration et de sécurité.

Le CERTA a pour mission de vous aider à répondre aux incidents de sécurité informatique.

Ne traitez pas les dysfonctionnements des machines à la légère. Dans certains incidents dans lesquels le CERTA intervient, les administrateurs des machines font spontanément part de petits dysfonctionnements inexpliqués et d'apparence anodine qui s'avèrent, au cours de l'analyse, être liés à un incident majeur de sécurité. N'hésitez pas à prendre contact avec le CERTA si vous constatez de l'activité sur les ports décrits ci-dessus.

4.7 Former et sensibiliser les utilisateurs

La sécurité d'un système d'information doit reposer sur une approche de défense en profondeur. Cela signifie, entre autres choses, que l'utilisateur est partie prenante de la sécurité. Sa vigilance, son niveau de formation et de sensibilisation participent à la sécurité du système. C'est pourquoi il est essentiel de prévoir des séances de formation et de sensibilisation des utilisateurs, acteurs de la sécurité. Pour vous aider dans ces actions, l'ANSSI dispose d'un centre de formation :

http://www.ssi.gouv.fr/site_rubrique62.html

Gestion détaillée du document

07 octobre 2011 version initiale.