Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 14 octobre 2011
N° CERTA-2011-ACT-041

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2011-41

Gestion du document

Référence	CERTA-2011-ACT-041
Titre	Bulletin d'actualité 2011-41
Date de la première version	14 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-041.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-041/

1 Mises à jour mensuelle Microsoft

Cette semaine, Microsoft a publié son ensemble mensuel de correctifs de sécurité. Ce sont ainsi huit bulletins de sécurité qui ont mis en ligne, corrigeant vingt trois vulnérabilités. Le CERTA rappelle l'impérative nécessité de déployer au plus vite ces mises à jour. Une synthèse des bulletins publiés est disponible dans la section Documentation ci-après.

Documentation

– Synthèse des bulletins de sécurité Microsoft du mois d'octobre 2011 :
http://technet.microsoft.com/fr-fr/security/bulletin/ms11-oct

2 Élévation de privilèges d'administrateur local à administrateur de domaine (3ème partie)

Nous continuons cette semaine l'énumération des moyens à la disposition des attaquants pour élever leurs privilèges dans le système d'information après l'exploitation réussie d'une vulnérabilité sur un poste ou sur un serveur.

Rapide : Extraire la base locale de sécurité, réutiliser les condensats

Attaque :

Depuis de nombreuses années, des techniques existent pour extraire les condensats de mots de passe de la base locale de sécurité (SAM). Ceux-ci ne permettront probablement pas d'obtenir des droits sur le domaine mais l'attaquant peut bénéficier de faiblesses courantes d'administration. En effet, le mot de passe utilisé pour un compte local peut être réutilisé pour un compte de domaine ou bien encore, un compte local privilégié peut être dupliqué sur un grand nombre de postes. L'attaquant aura alors l'opportunité de multiplier les attaques décrites ici et, dès lors, va considérablement augmenter ses chances de réussite.

Prévention :

La prévention de cette attaque consiste à s'assurer qu'un condensat de mot de passe local obtenu sur un poste ne puisse être réutilisé sur une autre machine ou sur le domaine. En l'espèce, il convient donc de s'assurer :

- que les mots de passe des comptes d'administration locaux ne sont pas réutilisés sur plusieurs postes. Ce type de situation est typiquement rencontré lors du déploiement d'images système sans réinitialisation des mots de passe ;
- que les mots de passe de comptes locaux ne sont pas réutilisés pour des comptes de domaine.

Lent : Casser les mots de passe locaux

Attaque :

Cette attaque est une variante (lente) de la précédente. Il s'agit encore d'une extraction des condensats de mots de passe de compte locaux mais cette fois à fin de « cassage ». L'objectif est désormais de retrouver les mots de passe en texte clair (en comparaison de la réutilisation du condensat de l'attaque précédente). Cette attaque va permettre à l'attaquant de retrouver les « habitudes » ou « formules » de création de mots de passe. Il aura alors la possibilité d'améliorer ses recherches de mots de passe utilisés dans l'entité attaquée.

Prévention :

Une méthode simple permet de prévenir cette attaque. Il faut (et il suffit) de ralentir l'attaque par dictionnaire et/ou par recherche exhaustive en utilisant un mot de passe suffisamment long et complexe pour empêcher toute déduction ou inférence à partir d'un mot de passe compromis.

3 Effet secondaire d'une mise à jour de box

3.1 Mise à jour avec régression

L'opérateur Orange a procédé à la mise à jour des boîtiers (*livebox*) déployés chez ses abonnés du 18 août au 19 septembre 2011. Malheureusement, pendant cette opération, le mot de passe d'administration est retourné à sa valeur initiale.

Le CERTA recommande de ne jamais conserver les mots de passes initiaux et de les remplacer dès installation, bien sûr par des mots de passe robustes. Cette recommandation s'applique également pour cette mise à jour.

De manière générale, il convient de vérifier que la mise à jour d'un logiciel ou d'un équipement ne crée pas une régression de configuration, par exemple la réinitialisation du mot de passe.

Le problème présent donne l'occasion à ceux qui n'avaient pas changé ce mot de passe de penser à le faire, et à ceux qui l'avait fait d'opter pour un autre mot de passe, le renouvellement périodique étant une bonne habitude.

L'opérateur a publié un article sur son site de support en ce sens (cf. Documentation).

3.2 Documentation

- Article du support Orange :
  http://assistance.orange.fr/livebox-mises-a-jour-1114.php
- Note d'information du CERTA *Les mots de passe* :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF001/
- Note d'information du CERTA *Acquisition des correctifs* :
  http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF004/

4 Rappel des avis émis

- CERTA-2011-AVI-551 : Vulnérabilité dans CyrusIMAPd
- CERTA-2011-AVI-552 : Vulnérabilité dans Microsoft Active Accessibility
- CERTA-2011-AVI-553 : Vulnérabilité dans Windows Media Center
- CERTA-2011-AVI-554 : Multiples vulnérabilités dans le sous-système win32k de Microsoft Windows
- CERTA-2011-AVI-555 : Vulnérabilité dans Microsoft NET Framework et Microsoft Silverlight
- CERTA-2011-AVI-556 : Vulnérabilités dans Microsoft Forefront Unified Access Gateway
- CERTA-2011-AVI-557 : Vulnérabilité dans Windows XP et Windows Server 2003
- CERTA-2011-AVI-558 : Multiples vulnérabilités dans Internet Explorer
- CERTA-2011-AVI-559 : Vulnérabilités dans Microsoft Host Integration Server
- CERTA-2011-AVI-560 : Vulnérabilités dans Cadic Intégrale
- CERTA-2011-AVI-561 : Vulnérabilité dans VLC
- CERTA-2011-AVI-562 : Vulnérabilité dans Apache mod_proxy
- CERTA-2011-AVI-563 : Vulnérabilité dans Apple pour iOS 15
- CERTA-2011-AVI-564 : Multiples vulnérabilités dans Apple Mac OS X
- CERTA-2011-AVI-565 : Multiples vulnérabilités dans Cisco Firewall Services Module
- CERTA-2011-AVI-566 : Multiples vulnérabilités dans Apple Safari
- CERTA-2011-AVI-567 : Vulnérabilités dans Apple iOS

5 Actions suggérées

5.1 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.

Quoi que 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.

5.2 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.

5.3 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.

5.4 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.

5.5 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.

5.6 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.

5.7 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

14 octobre 2011 version initiale.