Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 12 avril 2013
N° CERTA-2013-ACT-015

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2013-ACT-015

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-2013-ACT-015`

1 Mise à jour mensuelle Microsoft

Lors de la mise à jour mensuelle de Microsoft, neuf bulletins de sécurité ont été publiés.

Deux bulletins sont considérés comme critiques :
- MS13-028 qui concerne Microsoft Internet Explorer, cette mise à jour corrige deux vulnérabilités permettant à un attaquant, à l'aide d'une page Web spécialement conçue, d'exécuter du code arbitraire à distance ;
- MS13-029 qui concerne Microsoft Remote Desktop Client, cette mise à jour corrige une vulnérabilité permettant à un attaquant, à l'aide d'une page Web spécialement conçue, d'exécuter du code arbitraire à distance.

Sept bulletins sont considérés comme importants, ils concernent :
- une vulnérabilité dans Microsoft SharePoint (MS13-030) ;
- des vulnérabilités dans Microsoft Windows Kernel (MS13-031) ;
- une vulnérabilité dans Microsoft Active Directory (MS13-032) ;
- une vulnérabilité dans Microsoft CSRSS (MS13-033) ;
- une vulnérabilité dans Microsoft Windows Defender (MS13-034) ;
- une vulnérabilité dans Microsoft HTML Sanitization Component (MS13-035) ;
- des vulnérabilités dans Microsoft Kernel-Mode Driver (MS13-036).

Microsoft a constaté que le CVE-2013-1289 (MS13-035) a été utilisé dans des attaques ciblées, et que le CVE-2013-1290 (MS13-030) a été révélé publiquement.

Le CERTA recommande l'application de ces correctifs dès que possible.

Documentation

- Synthèse des bulletins de sécurité Microsoft du mois d'avril 2013 :
  `http://technet.microsoft.com/security/bulletin/ms13-apr`

2 Risques des applications de type gestionnaire de mots de passe

La multiplication des applications, et notamment des sites Web qui requièrent une authentification, accroît en permanence le nombre de mots de passe que l'utilisateur est contraint de gérer.

Face à cette tendance et par souci de facilité, les utilisateurs sont souvent tentés à réutiliser le même mot de passe entre les différents service qui en requièrent. Ce comportement est évidemment susceptible d'accroître les risques en cas de compromission d'un des services utilisés.

Une solution alternative consiste à utiliser une application permettant la sauvegarde sécurisée des mots de passe afin que l'utilisateur puisse s'affranchir de leur mémorisation.

Beaucoup d'applications de ce type qui existent, y compris pour les ordiphones, sont cependant loin d'être fiables. En effet, si certaines de ces applications annoncent dans leurs spécifications des niveaux et méthodes de chiffrement "militaires" (ex: certifications FIPS 140-2), la réalité est parfois toute autre.

A titre d'exemple, une étude a récemment démontré que l'application Keeper Password pour iOS, présentée comme une solution censée chiffrer les mots de passe avec l'algorithme de chiffrement AES, stockait en fait la base des mots de passe en clair sur l'ordiphone.

Il existe cependant des applications fiables comme c'est le cas de la solution libre KeePass Manager, certifiée CSPN dans sa version 2.10 Portable.

Le CERTA recommande l'utilisation d'applications de gestion de mots de passe certifiées et rappelle que l'emploi de ce type d'application ne dispense pas de l'utilisation de mots de passe robustes.

2.1 Documentation

- Rapport de Certification ANSSI-CSPN-2010/07
  http://www.ssi.gouv.fr/IMG/cspn/anssi-cspn_2010-07fr.pdf
- Recommandations de Sécurité Relatives aux Mots de Passe
  http://www.ssi.gouv.fr/IMG/pdf/NP_MDP_NoteTech.pdf
- Bullentin d'actualité CERTA-2013-ACT-014
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-ACT-014.pdf

3 Recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu

Une note technique de recommandations sur la définition d'une politique de filtrage réseau d'un pare-feu a été publiée par l'ANSSI le 05 avril 2013.

Le pare-feu est un des éléments majeurs de la sécurité des interconnections réseaux et la bonne définition de sa politique de filtrage est essentielle pour assurer une défense en profondeur efficace.

Il est fréquemment constaté que l'état des politiques de filtrage des pare-feux se dégrade naturellement avec le temps (méconnaissance de l'utilité de certaines règles, non suppression de règles liées à des équipements retirés de la production, etc.). De plus, la diversité des personnes qui administrent l'équipement peut conduire à une dérive de configuration (réutilisation d'adresses, règles surchargées, etc.). L'objectif du document est de fournir les éléments organisationnels pour structurer au mieux l'ensemble des règles de filtrage des pare-feux.

Le CERTA recommande la lecture et l'application des recommandations de cette note et de vérifier régulièrement que la politique de filtrage définie est bien appliquée.

Documentation

- Recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu :
  http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-des-r
  recommandations-pour-la-definition-d-une-politique-de-filtrage-reseau-d-un-pare.
  html

4 Recommandations de sécurité relatives aux réseaux Wifi

Une note technique de recommandations sur la sécurisation des réseaux Wifi a été publiée par l'ANSSI le 03 avril 2013.

L'utilisation des réseaux sans-fil Wifi est très répandue, tant chez les particuliers que dans le monde professionnel. Ces réseaux sont toutefois souvent peu sécurisés. Début 2013, il a été évalué que la moitié des réseaux Wifi n'utilisent aucun moyen de chiffrement ou utilisent un moyen de chiffrement obsolète. Pourtant, la bonne sécurisation de ces réseaux sans-fil est importante car ils peuvent permettre à des attaquants d'intercepter des données sensibles ou d'obtenir un point d'accès au système d'information.

Il est souvent possible de configurer assez simplement une borne Wifi pour avoir un paramétrage robuste et sécurisé. Les recommandations publiées permettent de guider le lecteur dans le choix des meilleurs paramètres pour la bonne sécurisation d'un réseau Wifi.

Le CERTA recommande la lecture de cette note technique et l'application des recommandations qu'elle contient à tous les points d'accès Wifi du système d'information.

Documentation

- Recommandations de sécurité relatives aux réseaux Wifi :
  http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-des-l
  recommandations-de-securite-relatives-aux-reseaux-wifi.html

5 Rappel des avis émis

Dans la période du 05 au 11 avril 2013, le CERTA a émis les publications suivantes :

- CERTA-2013-AVI-220 : Multiples vulnérabilités dans Opera
- CERTA-2013-AVI-221 : Multiples vulnérabilités dans PostgreSQL
- CERTA-2013-AVI-222 : Vulnérabilité dans Xen
- CERTA-2013-AVI-223 : Vulnérabilité dans Huawei AR
- CERTA-2013-AVI-224 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu
- CERTA-2013-AVI-225 : Multiples vulnérabilités dans Microsoft Internet Explorer
- CERTA-2013-AVI-226 : Vulnérabilité dans Microsoft Remote Desktop Client
- CERTA-2013-AVI-227 : Vulnérabilité dans Microsoft SharePoint
- CERTA-2013-AVI-228 : Multiples vulnérabilités dans Microsoft Windows Kernel
- CERTA-2013-AVI-229 : Vulnérabilité dans Microsoft Active Directory
- CERTA-2013-AVI-230 : Vulnérabilité dans Microsoft CSRSS
- CERTA-2013-AVI-231 : Vulnérabilité dans Microsoft Windows Defender
- CERTA-2013-AVI-232 : Vulnérabilité dans Microsoft HTML Sanitization Component
- CERTA-2013-AVI-233 : Multiples vulnérabilités dans Microsoft Kernel-Mode Driver
- CERTA-2013-AVI-234 : Multiples vulnérabilités dans Adobe ColdFusion
- CERTA-2013-AVI-235 : Multiples vulnérabilités dans Adobe Flash Player et AIR
- CERTA-2013-AVI-236 : Multiples vulnérabilités dans Adobe Shockwave Player
- CERTA-2013-AVI-237 : Multiples vulnérabilités dans Google Chrome
- CERTA-2013-AVI-238 : Multiples vulnérabilités dans Cisco IOS XE

- CERTA-2013-AVI-239 : Vulnérabilité dans Cisco Prime Network Control Systems
- CERTA-2013-AVI-240 : Multiples vulnérabilités dans Cisco FWSM
- CERTA-2013-AVI-241 : Multiples vulnérabilités dans Cisco ASA
- CERTA-2013-AVI-242 : Multiples vulnérabilités dans Cisco Unified MeetingPlace
- CERTA-2013-AVI-243 : Multiples vulnérabilités dans Oracle Solaris

Gestion détaillée du document

12 avril 2013 version initiale.