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 octobre 2012
N° CERTA-2012-ACT-041

**Affaire suivie par :**
CERTA

# BULLETIN D'ACTUALITÉ

## Objet : Bulletin d'actualité CERTA-2012-ACT-041



## Gestion du document

| | |
|---|---|
| Référence | CERTA-2012-ACT-041 |
| Titre | Bulletin d'actualité CERTA-2012-ACT-041 |
| Date de la première version | 12 octobre 2012 |
| 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.

## 1 Mises à jour mensuelles de Microsoft

Ce mois-ci, sept avis de sécurité ont été publiés dans le cadre des mises à jour menseulles de *Microsoft*. Nous attirons l'attention sur les vulnérabilités affectant *Microsoft Office Word*, considérées comme « critiques » par l'éditeur.

Les vulnérabilités corrigées permettent :

- de l'exécution de code arbitraire à distance ;
- l'atteinte à la confidentialité des données ;
- l'élévation de privilèges ;
- des dénis de services à distance ;
- et de l'injection de code indirecte à distance.

Le CERTA recommande l'application de ces mises à jour dès que possible.

### Documentation

- Synthèse des bulletins de sécurité Microsoft du mois de Septembre 2012 :
  http://technet.microsoft.com/fr-fr/security/bulletin/ms12-oct
- Alerte CERTA sur les vulnérabilités du produit Internet Explorer :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-ALE-006/index.html

## 2 Mises à jour consécutives de Mozilla Firefox

Le 9 octobre 2012, Mozilla a publié la version 16.0.0 de Mozilla Firefox. Cette nouvelle version corrigeait 13 vulnérabilités critiques. Ces vulnérabilités pouvaient être exploitées par un attaquant pour exécuter du code arbitraire à distance sans aucune interaction de l'utilisateur. En outre, le CERTA tient à souligner qu'à partir de cette version 16.0.0 de Mozilla Firefox, l'algorithme de hachage MD5 n'est plus accepté pour les signatures.

Le 11 octobre 2012, Mozilla publie la version 16.0.1 de Mozilla Firefox. Cette nouvelle version corrige une régression constatée dans Mozilla Firefox 16.0.0. Cette régression est une vérification qui n'est pas faite dans la méthode *defaultValue*. Elle permet à un attaquant d'effectuer des actions, souvent silencieuses, sur un autre domaine Internet que celui visité. Ce type de faille est principalement utilisé pour proliférer du code malveillant sur des sites communautaires ou pour récupérer des informations confidentielles de l'utilisateur.

Le CERTA recommande aux utilisateurs de mettre à jour rapidement le navigateur Mozilla Firefox en version 16.0.1.

**Documentation**

- Notes de version Firefox 16.0.1 :
  http://www.mozilla.org/en-US/firefox/16.0.1/releasenotes/
- Notes de version Firefox 16.0.0 :
  http://www.mozilla.org/en-US/firefox/16.0/releasenotes/
- Vulnérabilité dans Firefox 16.0.0 :
  https://blog.mozilla.org/security/2012/10/10/security-vulnerability-in-firefox-16/
- MD5 n'est plus accepté comme algorithme de hachage pour les signatures :
  https://bugzilla.mozilla.org/show_bug.cgi?id=650355

## 3 Des équipements réseau parfois négligés, mais cruciaux pour la sécurité

Lorsqu'il est question de maintenir à jour des systèmes à des fins de sécurité, il est parfois constaté que des équipements réseau sont, à tort, négligés. Pourtant, la compromission d'un des ces équipements peut avoir un impact très important sur la sécurité des réseaux. C'est notamment le cas des routeurs ou modems DSL.

Un exemple a été dévoilé récemment par Fabio Assolini, un chercheur travaillant chez Kaspersky Lab. Il décrit dans un article (cf. Documentation) comment plus de 4 millions de modems DSL ont été compromis au Brésil, ainsi que les conséquences de ces compromissions. Une grande partie des modems DSL distribués au Brésil partageaient une vulnérabilité similaire, située dans le *firmware*, qui permettait de se connecter à distance à l'interface d'administration de l'équipement sans connaître au préalable le mot de passe. C'est en exploitant cette vulnérabilité que des attaquants ont eu accès à des modems DSL, appartenant à des particuliers ou des professionnels, puis ont modifié leur configuration en changeant notamment l'adresse du serveur DNS à utiliser. En dirigeant les requêtes DNS vers un serveur qu'ils contrôlaient, les attaquants avaient la possibilité de rediriger tout utilisateur demandant un site connu et réputé fiable vers un site Web malveillant.

Les méthodes de mise à jour de tels équipements varient fortement selon les constructeurs et peuvent se révéler complexes. Le CERTA rappelle toutefois l'importance de prendre en compte tout équipement réseau dans le processus de mise à jour et, plus généralement, dans l'évaluation de la sécurité d'un réseau. Cela implique notamment le suivi des bulletins de sécurité relatifs à ces équipements et l'application des correctifs disponibles.

**Documentation**

- Article de Fabio Assolini sur les compromissions de modems DSL au Brésil :
  http://www.securelist.com/en/blog/208193852/The_tale_of_one_thousand_and_one_DSL_modems

## 4 Annonce de nouveau standard SHA-3

Le NIST a annoncé le 2 octobre 2012 le résultat de la compétition SHA-3. La fonction de hachage Keccak, conçue par G. Bertoni, J. Daemen, G. Van Assche de ST Microelectronics et M. Peeters de NXP Semiconductors, a été choisie comme nouveau standard.

Cette compétition, lancée en 2007, était motivée par une série d'attaques découvertes en 2005. Ces attaques ont permis de « casser » la plupart des fonctions existantes, comme MD5 ou SHA-1 et ont jeté un doute sur la sécurité à long terme de SHA-2, dont les principes de conception sont assez similaires à SHA-1.

Cependant, SHA-2 a jusqu'à aujourd'hui bien résisté aux tentatives de cryptanalyse. Le nouveau standard SHA-3 n'a donc pas vocation à remplacer SHA-2 dans l'immédiat, mais à coexister avec cette fonction et à offrir une solution de repli au cas où SHA-2 viendrait à être compromis. Comme SHA-2, SHA-3 permet le calcul d'empreintes de 224, 256, 384 et 512 bits.

De ce fait, le choix du NIST s'est porté sur une fonction offrant un profil très complémentaire de celui de SHA-2. Keccak repose sur des principes de conception différents de ceux de SHA-2 et de ces prédecesseurs, tant au niveau de la structure générale que des opérations élémentaires utilisées. Ces nouveaux principes rendent improbable la découverte d'une attaque affectant ces ceux fonctions à la fois. Dix ans de tentatives infructueuses pour attaquer SHA-2 ont renforcé la confiance qu'on peut accorder à cette fonction. Toutefois, Keccak a bénéficié d'une meilleure connaissance des techniques d'attaques potentielles lors de sa conception et dispose d'une grande marge de sécurité. Ces deux fonctions offrent donc un bon niveau de sécurité par rapport à l'état de l'art.

Les implantations matérielles de Keccak peuvent offrir des débits élevés ou une bonne résistance aux attaques par canaux auxiliaires, alors que SHA-2 peut être implémenté de manière légèrement plus compacte. En implémentation logicielle, du fait du type d'instructions utilisées, SHA-2 permet d'obtenir de meilleurs débits.

Les fonctions de hachage sont utilisées par de nombreux mécanismes cryptographiques tels que la signature électronique, le calcul de motifs d'intégrité de messages, la génération de nombres aléatoires, les fonctions de dérivation de clés ou encore le stockage des mots de passe.

**Documenation**

– Annonce du vainqueur de la compétition SHA-3 par le NIST le 2 octobre 2012 :
http://csrc.nist.gov/groups/ST/hash/sha-3/winner_sha-3.html

# 5 Recommandations de sécurité relatives à IPsec

La technologie IPsec permet de protéger efficacement la confidentialité et l'intégrité de toutes sortes de flux transitant sur des réseaux IP. Elle est disponible nativement sur beaucoup d'équipements réseau ainsi que sur les principaux systèmes d'exploitation, à la fois pour les postes de travail, les serveurs ou les terminaux mobiles.

Plusieurs solutions d'accès à distance à un réseau reposent sur IPsec. Elles sont donc couramment utilisées pour répondre aux problématiques de mobilité. Le champ d'application d'IPsec va toutefois bien au-delà de ce sujet et s'étend aussi bien aux réseaux locaux au sein des centres serveurs qu'aux liaisons entre les différents établissements d'un organisme.

L'ANSSI a récemment publié un guide destiné à mieux faire connaître IPsec et à comprendre comment cette solution peut améliorer notablement la sécurité de nombreux systèmes sans exiger d'investissements lourds (cf. documentation).

**Documentation**

– Recommandations de sécurité relatives à IPsec :
http://www.ssi.gouv.fr/IMG/pdf/NP_IPsec_NoteTech.pdf

# 6 Recommandations de sécurité relatives à la télé-assistance

L'ANSSI a récemment publié une note technique de recommandations de sécurité relatives à la télé-assistance (cf. documentation).
Cette note traite en particulier de la fonctionnalité *assistance à distance* de Microsoft et de la suite VNC.

Largement utilisées pour répondre à des problématiques de réactivité et de ressources humaines, les solutions de télé-assistance ne sont pas exemptes de vulnérabilités (cf. les nombreux avis et alertes publiées régulièrement par le CERTA sur ces technologies).

Le CERTA ne peut qu'inciter ses lecteurs à appliquer les recommandations préconisées dans cette note, afin de limiter l'exposition des réseaux et postes sur lesquels ces technologies sont employées.

**Documentation**

– Recommandations de sécurité relatives à la télé-assistance :
http://www.ssi.gouv.fr/IMG/pdf/NP_Teleassistance_NoteTech.pdf

# 7 Rappel des avis émis

Dans la période du 05 au 11 octobre 2012, le CERTA a émis les publications suivantes :

– CERTA-2012-AVI-545 : Multiples vulnérabilités dans Wireshark
– CERTA-2012-AVI-546 : Multiples vulnérabilités dans Apple OS X Server
– CERTA-2012-AVI-547 : Vulnérabilité dans HP Network Node Manager i (NNMi)
– CERTA-2012-AVI-548 : Multiples vulnérabilités dans VMware
– CERTA-2012-AVI-549 : Vulnérabilités dans IBM Lotus Notes Traveler
– CERTA-2012-AVI-550 : Vulnérabilité dans le système SCADA Siemens SIMATIC S7-1200
– CERTA-2012-AVI-551 : Multiples vulnérablilités dans Google Chrome
– CERTA-2012-AVI-552 : Vulnérabilités dans IBM Tivoli Directory Server
– CERTA-2012-AVI-553 : Multiples vulnérabilités dans Adobe Flash Player
– CERTA-2012-AVI-554 : Vulnérabilités dans Microsoft Office
– CERTA-2012-AVI-555 : Vulnérabilité dans Microsoft Works
– CERTA-2012-AVI-556 : Vulnérabilité dans le composant de nettoyage HTML de Microsoft
– CERTA-2012-AVI-557 : Multiples vulnérabilités dans FAST Search Server
– CERTA-2012-AVI-558 : Vulnérabilité dans le noyau Microsoft Windows
– CERTA-2012-AVI-559 : Vulnérabilité dans Kerberos de Microsoft
– CERTA-2012-AVI-560 : Vulnérabilité dans Microsoft SQL Server
– CERTA-2012-AVI-561 : Multiples vulnérabilités dans les produits Mozilla
– CERTA-2012-AVI-562 : Vulnérabilité dans RSA Adaptative Authentication
– CERTA-2012-AVI-563 : Multiples vulnérabilités dans Pale Moon
– CERTA-2012-AVI-564 : Multiples vulnérabilités dans Cisco ASA
– CERTA-2012-AVI-565 : Vulnérabilité dans Joomla!
– CERTA-2012-AVI-566 : Vulnérabilités dans HP Secure Web Server
– CERTA-2012-AVI-567 : Multiples vulnérabilités dans Cisco Firewall Services Module
– CERTA-2012-AVI-568 : Multiples vulnérabilités dans Cisco WebEx
– CERTA-2012-AVI-569 : Vulnérabilité dans ISC BIND

# 8 Actions suggérées

## 8.1 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.

## 8.2 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.

## 8.3 Appliquer les correctifs de sécurité

Le CERTA recommande l'application des correctifs de sécurité.

## 8.4 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.

## 8.5 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.

## 8.6 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.

## 8.7 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

**12 octobre 2012** version initiale.