Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 30 décembre 2011
N° CERTA-2011-ACT-052

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2011-52

Gestion du document

Référence	CERTA-2011-ACT-052
Titre	Bulletin d'actualité 2011-52
Date de la première version	30 décembre 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-052.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-052/

1 Bilan de l'année

L'année 2011 s'achève. Naturellement, c'est donc le moment des bilans et des bonnes résolutions ! Comme tous les ans, l'année a été particulièrement riche dans le domaine de la SSI. Cette année, le traitement d'infections de grandes ampleurs au sein de réseaux (administration, OIV, ...) constitue probablement un tournant important dans nos activités. Sans partir dans des élucubrations, il s'agit, dans de nombreux cas traités, d'affaires d'espionnage industriel ou économique de grandes ampleurs. Les attaquants compromettent puis s'installent durablement dans les réseaux afin de collecter toutes les données qui les intéressent.

L'année 2011 a aussi été marquée par une augmentation du nombre d'avis publiés par le CERTA. Pas moins de 730 avis et 8 alertes ont ainsi été diffusés. Les attaques exploitant des vulnérabilités présentes dans les formats bureautiques ont encore eu beaucoup d'impacts. Le CERTA a pu constater dans les incidents qu'il est amené à traiter la forte augmentation d'attaques par le biais de fichiers PDF. Aussi, en cette fin d'année, il ne faut pas relâcher sa vigilance lors de l'ouverture de certains courriels et des traditionnelles cartes de vœux électroniques. Il est important de noter qu'à la date d'écriture de cet article, une alerte est toujours en cours sur une faille PDF critique non corrigée dans les produits Adobe Acrobat X et Adobe Reader X (CERTA-2011-ALE-008).

Les attaques visant l'atteinte à la disponibilité (déni de service) ont aussi été pléthoriques cette année. Il est important dans notre domaine de pouvoir anticiper de telles menaces. La protection contre les attaques en DDoS

(déni de service distribué) illustre parfaitement ce principe, car si des solutions de protection existent et sont maintenant relativement matures, elles sont toutefois extrêmement complexes à mettre en œuvre dans le feu de l'action et doivent donc être impérativement anticipées.

D'un point de vue plus organisationnel, l'Agence nationale de la sécurité des systèmes d'information (ANSSI), dont le CERTA fait partie, continue sa croissance. Le CERTA rappelle que des postes sont toujours à pourvoir au sein de l'équipe et plus largement au sein de l'ANSSI. Les offres d'emploi sont disponibles à l'adresse suivante :
http://www.ssi.gouv.fr/fr/anssi/emploi/

Le bulletin d'actualité est, pour le CERTA, le moyen de partager sa vision et son expérience en matière de traitement d'incident. Les retours sur cette production sont toujours fortement appréciés. N'hésitez donc pas à nous faire part de vos remarques. Il ne nous reste plus qu'à vous souhaiter une excellente fin d'année 2011 et une bonne année 2012 et à vous donner rendez-vous l'année prochaine pour continuer ensemble l'effort global de sécurisation de nos systèmes d'information. Très bonne et heureuse année à toutes et à tous !

2 Vulnérabilité dans certains démons et clients Telnet

Bien qu'assez ancien, le protocole Telnet reste tout de même relativement utilisé, notamment dans le cadre de l'administration distante d'équipement réseau. Aussi, une vulnérabilité touchant un démon ou un client Telnet représente une réelle menace.

La vulnérabilité CVE-2011-4862 touchant le démon Telnet installé par défaut sur FreeBSD, divulguée le 25 décembre de cette année, représente donc un bien beau cadeau de Noël pour les attaquants. En effet, cette vulnérabilité permet de prendre le contrôle complet d'une machine distante (invite de commande root) utilisant ce démon et ce sans authentification.

De plus, il s'avère que cette vulnérabilité touche aussi d'autres implémentations de Telnet. En effet, le module vulnérable est utilisé dans d'autres implémentations. C'est le cas notamment du démon Telnet inclus dans MIT Kerberos (versions 5 et antérieures) ainsi que dans le package *inetutils*.

Pire, certains clients, lorsqu'ils sont compilés avec les options de prise en compte de la cryptographie, sont aussi vulnérables. Ainsi, une connexion sur un faux serveur Telnet peut conduire un attaquant à prendre le contrôle complet de la machine client.

D'un point de vue technique, la fonction fautive `encrypt_keyid`, située dans le fichier *encrypt.c*, est vulnérable à un dépassement de tampon lors de la réception des options de négotiation de la clé cryptographique. Ce type de vulnérabilité, bien connu, est relativement simple à exploiter. Des codes d'exploitation fonctionnels sont d'ailleurs disponibles librement sur Internet.

Le CERTA recommande donc une grande vigilance vis-à-vis de cette vulnérabilité. Il est notamment conseillé aux utilisateurs de FreeBSD n'ayant pas besoin d'un serveur Telnet de le désactiver. Il est aussi préférable d'utiliser des versions du client Telnet ne supportant pas les options cryptographiques, dans le cas où de la cryptographie n'est pas nécessaire (c'est par exmenple le cas du client Telnet disponible sur un installation Debian de base). Un correctif est par ailleurs disponible. Cependant, ce dernier n'est pour l'instant présent que dans les dépôts des différents éditeurs, les versions binaires devraient suivre sous peu.

3 Déni de service HashDOS

Une nouvelle technique pour réaliser un déni de service sur un site Internet a été présentée à la conférence 28c3 (28th Chaos Communication Congress) à Berlin. Cette technique utilise une faille de conception présente dans la plupart des langages de programmation Web (PHP, Python, Ruby, ASP.NET, Java...). Lors du traitement d'une requête, un condensat simple de chaque paramètre est réalisé. La mise en base des condensats d'un grand nombre de paramètres est normalement très rapide. Cependant, s'il y a un grand nombre de collisions dans les condensats la vitesse de mise en base est beaucoup plus lente.

L'attaque consiste donc à envoyer au serveur des requêtes très longues, contenant de très nombreux paramètres qui ont tous le même condensat ; ces paramètres sont relativement faciles à calculer pour l'attaquant car il ne s'agit pas de condensats cryptographiques forts. Selon les calculs effectués par les chercheurs, 500ko de requêtes spécialement conçues engendrent une minute de temps de traitement sur un serveur PHP muni d'un processeur *Intel Core i7*. Avec un débit de moins de 100kbits/s un attaquant peut occuper à 100% un serveur PHP muni d'un processeur *Intel Core i7*. Avec un débit de 6kbits/s un attaquant peut occuper à 100% un serveur Java+Tomcat muni d'un processeur *Intel Core i7*.

Une fois un important volume de données engendrant le même condensat calculé pour un langage donné, il peut être utilisé pour attaquer n'importe quel serveur utilisant ce langage, et être très facilement diffusé sur Internet.

Des mises à jour ont été publiées, qui permettent aux administrateurs de site de mettre en place des solutions de contournement : limiter la taille des requêtes acceptées, limiter le nombre de paramètres acceptables dans une requête. Une autre solution de contournement est de limiter le temps processeur disponible par fil d'exécution.

Le CERTA recommande d'installer ces mises à jour au plus tôt et d'adapter les nouveaux paramètres aux besoins.

Documentation :

- Présentation faite lors de la 28c3 :
  http://events.ccc.de/congress/2011/Fahrplan/events/4680.en.html
- Avis de sécurité nruns du 28 décembre 2011 :
  http://www.nruns.com/_downloads/advisory28122011.pdf

4 Rappel des avis émis

Dans la période du 23 décembre au 29 décembre 2011, le CERTA a émis les publications suivantes :

- CERTA-2011-AVI-717 : Vulnérabilités dans Moodle
- CERTA-2011-AVI-718 : Vulnérabilité dans telnetd sur FreeBSD
- CERTA-2011-AVI-719 : Vulnérabilité dans phpMyAdmin
- CERTA-2011-AVI-720 : Vulnérabilité dans phpMyAdmin
- CERTA-2011-AVI-721 : Multiples vulnérabilités dans HP Managed Printing Administration
- CERTA-2011-AVI-722 : Vulnérabilité dans pam_ssh sur FreeBSD
- CERTA-2011-AVI-723 : Multiples vulnérabilités dans les produits Websense
- CERTA-2011-AVI-724 : Vulnérabilité dans IBM Lotus Domino
- CERTA-2011-AVI-725 : Vulnérabilité dans IBM DB2
- CERTA-2011-AVI-726 : Multiples vulnérabilités dans F5 Enterprise Manager

Durant la même période, les publications suivantes ont été mises à jour :

- CERTA-2011-ALE-007-001 : Vulnérabilité dans ftpd et ProFTPD sur FreeBSD (ajout des correctifs FreeBSD)
- CERTA-2011-AVI-706-001 : Vulnérabilité dans OpenPAM (ajout des correctifs FreeBSD)

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.

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.

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

30 décembre 2011 version initiale.