Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 03 juin 2011
N° CERTA-2011-ACT-022

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2011-22

Gestion du document

Référence	CERTA-2011-ACT-022
Titre	Bulletin d'actualité 2011-22
Date de la première version	03 juin 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-022.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-022/

1 Vol de cookies, une menace non négligeable

1.1 Qu'est-ce qu'un *cookie* ?

Dans le langage informatique, un *cookie* est défini comme étant une donnée binaire opaque, c'est à dire une donnée qui n'a pas de sens pour la personne qui la détient mais qui en a pour son émetteur. D'un point de vue allégorique, un *cookie* peut être représenté par un ticket de vestiaire : le ticket en lui-même n'a pas de sens pour la personne déposant son manteau mais permet au service de vestiaire de retrouver la veste déposée, grâce aux informations qu'il contient (un numéro de vestiaire).

Sur l'Internet, les *cookies* sont très largement utilisés. Ils permettent par exemple à un serveur de stocker des informations de configuration sur un poste : le client pourra ensuite se reconnecter en présentant ce *cookie* au serveur, qui appliquera alors les préférences enregistrées. Bien entendu, de nombreux autres types de *cookies* existent.

Le plus répandu est certainement le *cookie* de session HTTP, émis lors de l'identification d'un client sur un site Internet. Il permet à l'utilisateur authentifié de naviguer sur le site sans avoir à saisir de nouveau son mot de passe : la présentation du *cookie* suffit.

1.2 Le vol de *cookie*

Comme nous venons de le voir, les *cookies* peuvent être utilisés afin d'identifier un compte. Imaginons alors qu'un attaquant puisse, par un moyen quelconque, récupérer le *cookie* d'identification d'un utilisateur. Il pourrait ensuite utiliser ce *cookie* pour effectuer des actions avec les privilèges et sous l'identité de cet utilisateur.

Bien entendu, l'accès à un *cookie* stocké sur une machine n'est pas trivial et plusieurs mécanismes de sécurité rendent difficile sa lecture par un utilisateur malveillant ou un site frauduleux. Notamment grâce à la mise en place d'une politique de cloisonnement des domaines : un *cookie* ne peut être présenté qu'au domaine qui l'a émis.

Cependant, il existe des méthodes basées sur divers types de failles (notamment XSS et CSRF) qui permettent à un attaquant de voler des *cookies* d'authentification.

Outre ces techniques classiques, un expert en sécurité a récemment découvert une faille dans *Internet Explorer* permettant de passer outre la politique de restriction inter-domaine. Il s'est en effet rendu compte qu'une erreur de mise en œuvre dans la *Cross zone interaction policy* (une politique interdisant aux pages Web d'accéder au système de fichiers de la machine) permet d'afficher le contenu de n'importe quel *cookie* dans une *iframe*. Bien que cette faille soit extrêmement dangereuse, sa puissance est limitée par un problème de taille : comment extraire les informations contenues dans les *cookies* ? En effet, même si la politique d'accès inter-domaine au *cookie* est contournée, l'*iframe* contenant les informations n'est pas un objet contrôlé par l'attaquant : son accès est bloqué par la *Same Origin Policy*.

Cependant, le découvreur montre qu'il est possible d'utiliser des techniques avancées de *clickjacking* afin de pousser l'utilisateur à rendre ces informations accessibles à l'attaquant.

1.3 Conclusion

Comme nous venons de le voir, les techniques de vol de *cookies* évoluent et se modernisent. Il est donc nécessaire de sensibiliser les utilisateurs à ce type de menaces et aux bonnes pratiques liées à la navigation sur l'Internet.

Documentation

- Cookiejacking :
  http://sites.google.com/site/tentacoloviola
- Http cookie :
  http://fr.wikipedia.org/wiki/Cookie_(informatique)
- Clickjacking :
  http://fr.wikipedia.org/wiki/Clickjacking
- Note d'information CERTA-2002-INF-001 sur la vulnérabilité de type « Cross Site Scripting » :
  http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-001
-
- Note d'information CERTA-2008-INF-003 sur les attaques de type « cross-site request forgery » :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-INF-003

2 Vulnérabilité dans certains services installés sous Debian

Lorsqu'ils sont démarrés sur un système UNIX, certains démons conservent leur numéro de processus (ou *PID*) dans un fichier stocké dans un répertoire particulier.

Dans une distribution Debian, il est d'usage que ces fichiers soient stockés dans le répertoire */var/run*. Or il a été découvert que certains démons, une fois démarrés, créent ces fichiers avec des permissions trop laxistes. Par exemple, ceux-ci pourront être modifiés par n'importe quel utilisateur malveillant.

Or ces fichiers sont utilisés par les administrateurs systèmes, ou des scripts automatiques pour identifier les processus appartenant au démon afin de recharger sa configuration en lui envoyant un signal POSIX adapté.

Un utilisateur malveillant pourra donc modifier ces fichiers pour que ces signaux ou commandes soient envoyés à un autre processus.

À la date d'écriture de cet article, seuls les services *keepalived* et *openswan* ont été reconnus comme touchés par cette vulnérabilité, identifiée respectivement par leur numéro CVE : CVE-2011-1784 et CVE-2011-2147. Un courriel à la liste debian-security semble montrer que d'autres services utilisés, entre autre, pour la gestion du protocole IPsec posent le même problème de sécurité.

Le CERTA conseille donc de vérifier les permissions de ces fichiers. La vulnérabilité peut toucher tout logiciel qui stocke son numéro de processus dans un fichier dont les permissions sont trop ouvertes, quelque soit le système compatible POSIX utilisé.

Documentation

- Discussion sur la liste de diffusion debian-security :
  http://lists.debian.org/debian-security/2011/05/msg00012.html
- Statut de la vulnérabilité CVE-2011-1784 affectant keepalived dans Debian :
  http://security-tracker.debian.org/tracker/CVE-2011-1784
- Statut de la vulnérabilité CVE-2011-2147 affectant openswan dans Debian :
  http://security-tracker.debian.org/tracker/CVE-2011-2147
- Référence CVE CVE-2011-1784 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1784
- Référence CVE CVE-2011-2147 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2147

3 Outils d'analyse antivirale hors-ligne

Microsoft vient de publier cette semaine une version Bêta de Microsoft Standalone System Sweeper. Cet outil vous permet de créer un CD, une clé USB ou une image ISO « *bootable* » et de scanner un système hors-ligne. Le moteur et les signatures sont les mêmes que ceux utilisés par Microsoft Security Essential ou Forefront Security.

Ces outils ne remplacent pas un antivirus mais peuvent s'avérer utiles lors d'une analyse à froid (en mode détection) d'un système infecté ou en complément ponctuel dans certains cas d'infection.

D'autres outils de ce type existent déjà, vous en trouverez une liste (non exhaustive) dans la section Documentation.

Documentation

- Microsoft Standalone System Sweeper Beta :
  http://connect.microsoft.com/systemsweeper
- Kaspersky Rescue Disk 10 :
  http://support.kaspersky.com/viruses/rescuedisk
- F-secure Rescue CD :
  http://www.f-secure.com/en_EMEA-Labs/security-threats/tools/rescue-cd
- Avira AntiVir Rescue System :
  http://www.avira.com/en/support-download-avira-antivir-rescue-system
- Norton Bootable Recovery Tool :
  http://security.symantec.com/nbrt/nbrt.aspx?lcid=1033&origin=default

4 Liens utiles

- Mémento sur les virus :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-002/
- Note d'information du CERTA sur l'acquisition de correctifs :
  http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-004/
- Note d'information du CERTA sur les systèmes obsolètes :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-003/
- Note d'information du CERTA sur les bonnes pratiques concernant l'hébergement mutualisé :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005/
- Note d'information du CERTA sur les mots de passe :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/
- Note d'information sur la terminologie d'usage au CERTA :
  http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-002/

– Note d'information du CERTA sur les enjeux de sécurité liés à une migration vers IPv6 : http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-004/
– Unix security checklist version 2.0 du 8 octobre 2001 (Publication du CERT australien) : http://www.auscert.org.au/render.html?it=1937
– Note d'information du CERTA sur les risques associés aux clés USB : http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-006/
– Note d'information du CERTA sur les outils d'indexation et de recherche : http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-009/
– Note d'information du CERTA sur la gestion des noms de domaine : http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-001/
– Note d'information du CERTA sur le bon usage de PHP : http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-002/

5 Rappel des avis émis

Dans la période du 28 mai au 02 juin 2011, le CERTA a émis les publications suivantes :

– CERTA-2011-AVI-317 : Vulnérabilités dans GRR
– CERTA-2011-AVI-318 : Vulnérabilités dans WordPress
– CERTA-2011-AVI-319 : Vulnérabilité dans Symantec Backup Exec
– CERTA-2011-AVI-320 : Vulnérabilité dans Bind
– CERTA-2011-AVI-321 : Multiples vulnérabilités dans Drupal
– CERTA-2011-AVI-322 : Vulnérabilité dans IBM Tivoli
– CERTA-2011-AVI-323 : Vulnérabilité dans Zope

6 Actions suggérées

6.1 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.

6.2 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.

6.3 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.

6.4 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.

6.5 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.

6.6 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.

6.7 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

7 Les bulletins d'actualité

L'objectif des *bulletins d'actualité* est de fournir une illustration par l'actualité récente de certaines mesures de sécurité pragmatiques à appliquer. Bien que par nature *a posteriori*, cette illustration a vocation à servir de base pour tirer des enseignements plus généraux à même de protéger contre des incidents futurs.

L'« actualité » est donnée par l'analyse de machines que le CERTA réalise dans le cadre de ses missions. Un fait est jugé d'actualité, s'il est à la fois récent et significatif, c'est à dire recoupé par différentes analyses.

Les *bulletins d'actualité* n'ont pas la prétention de constituer des statistiques fiables de l'activité informatique malveillante, mais ce qui nous semble avoir beaucoup plus d'intérêt, de montrer à partir d'exemples concrets, réels et anonymisés comment découvrir que l'on est ou a été attaqué et comment limiter l'impact de ces attaques.

La qualité des *bulletins d'actualité* sera améliorée grâce à votre participation. Si vous souhaitez participer, prenez contact avec le CERTA en accord avec votre chaîne fonctionnelle de la sécurité des systèmes d'information.

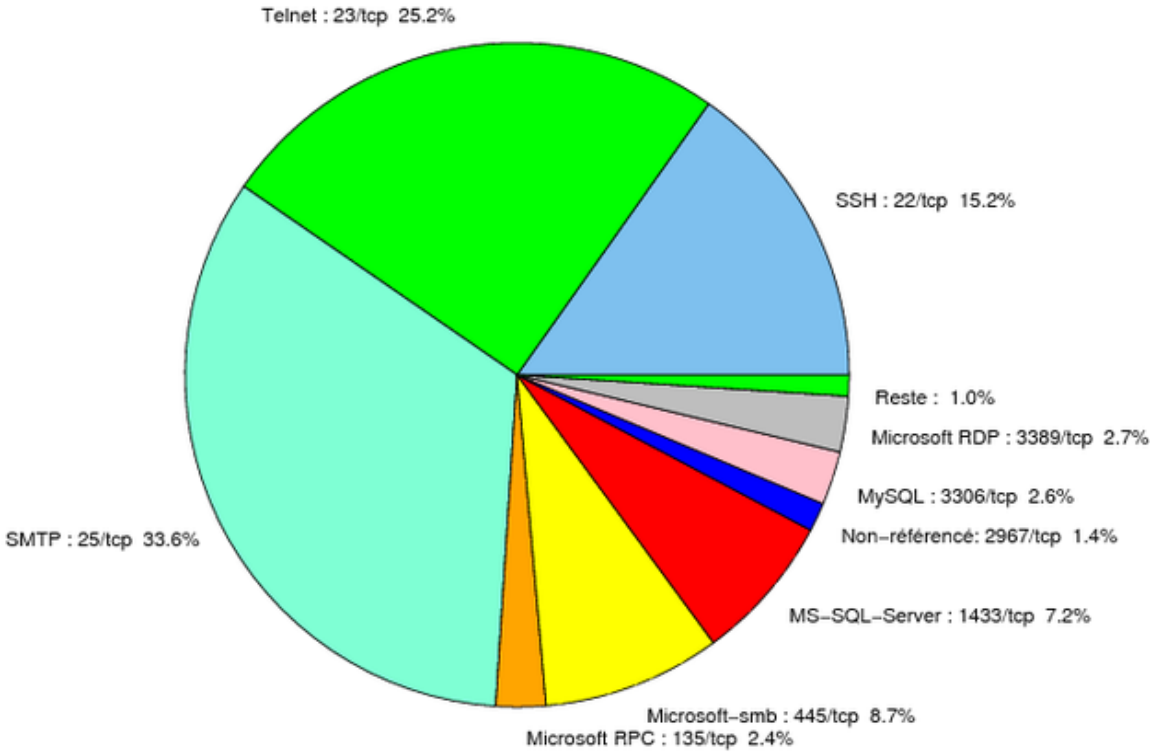

FIG. 1: Répartition relative des ports pour la semaine du 28 mai au 02 juin 2011

port	pourcentage
25/tcp	33.58
23/tcp	25.18
22/tcp	15.2
445/tcp	8.67
1433/tcp	7.18
80/tcp	7.08
3389/tcp	2.7
3306/tcp	2.61
135/tcp	2.42
2967/tcp	1.39
3128/tcp	0.46
21/tcp	0.37
1080/tcp	0.18

TAB. 2: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

03 juin 2011 version initiale.