

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2010-49

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-2010-ACT-049>

Gestion du document

Référence	CERTA-2010-ACT-049
Titre	Bulletin d'actualité 2010-49
Date de la première version	10 décembre 2010
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-2010-ACT-049.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-2010-ACT-049/>

1 Incident de la semaine

Filoutages de messageries professionnelles

1.1 Les faits

Plusieurs services clients du CERTA ont fait récemment face à des filoutages contre leurs messageries professionnelles. Des utilisateurs ont reçu un courriel prétendant émaner du service informatique et demandant au destinataire son identifiant et son mot de passe de connexion à la messagerie professionnelle.

La capture de ces informations sensibles peut se faire par demande de réponse à l'expéditeur du message ou par insertion dans le courriel d'un lien vers un site imitant le site de l'organisme.

L'un des cas signalés au CERTA ne s'est pas cantonné à une simple fuite d'identifiants mais a eu des répercussions sur tout le service. Les rares utilisateurs naïfs qui ont répondu aux sirènes de ces messages ont vu leurs comptes immédiatement utilisés pour des campagnes de pourriels. La conséquence rapide a été l'inscription du serveur de messagerie de leur service dans certaines listes noires. Les courriels légitimes de *tous* les agents du service étaient alors susceptibles d'être rejetés par les serveurs de messagerie qui se reposent sur les listes noires qui ont inscrit ce serveur.

La sortie de certaines listes noires à la demande d'un administrateur de messagerie qui a pris les mesures correctives nécessaires est parfois laborieuse ou onéreuse.

1.2 Recommandations

Au niveau de l'organisation, il est impératif de prévenir les utilisateurs des modalités de communication des services de support aux utilisateurs, et de répéter que les demandes d'identifiant et de mots de passe par messagerie sont *a priori* malveillantes. Cette communication doit être répétée régulièrement, afin que les nouveaux utilisateurs bénéficient de cette mise en garde. Se rapprocher du service des ressources humaines pour connaître les périodes de forte embauche permet d'optimiser cette communication.

Les utilisateurs doivent également s'imprégner des bonnes habitudes et ne pas penser que les conséquences se limitent à leur seul compte de messagerie. La note d'information du CERTA « Mesures de prévention relatives à la messagerie » (voir section Documentation) pourra aider à la rédaction d'une communication pour faire prendre ces bonnes habitudes. Les bonnes pratiques peuvent être inscrites dans la PSSI mais également dans un livret d'accueil, lorsque celui-ci existe pour les nouveaux arrivants.

Lorsqu'un utilisateur est tombé dans le piège d'un filoutage, il faut l'inciter à changer *tous* les mots de passe qu'il utilise dans le SI. Trop souvent ces mots de passe sont en fait identiques et changer le mot de passe de messagerie qui a été divulgué ne met pas à l'abri les autres accès au SI.

Par ailleurs, si les listes noires peuvent être utilisées pour éliminer du trafic indésirable, il est préférable d'utiliser des listes dont le processus d'entrée et de sortie de liste noire est transparent. Il est également souhaitable de pouvoir mettre des listes blanches de serveurs ou d'adresses IP, de sorte que, si un interlocuteur habituel est en liste noire à tort ou accidentellement, les courriels légitimes que ce dernier émet ne soient pas rejetés.

1.3 Documentation

- Document du CERTA CERTA-2000-INF-002, Mesures de prévention relatives à la messagerie : <http://www.certa.ssi.gouv.fr/site/CERTA-200-INF-002/index.html>
- Document du CERTA CERTA-2005-INF-001, Les mots de passe : <http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/index.html>

2 Exim dans Debian

Cette semaine a été publiée une vulnérabilité relative à la version 4.69 du serveur de messagerie Exim pouvant aboutir à une exécution de code arbitraire à distance par le biais d'un message construit de façon particulière. Or, la dernière version à la date du présent article est la 4.72. Cette faille n'a donc pas donné lieu à une publication d'avis par le CERTA. Cependant, la version 4.69 est celle présente avec la distribution GNU/Linux Debian stable nommée Lenny et pour le moment, le paquetage associé n'est, d'ailleurs, pas corrigé dans cette distribution.

Recommandation

Exim est employé dans la distribution Debian comme l'agent de messagerie par défaut. Il conviendra donc, d'appliquer au plus vite le correctif (Cf. le bulletin de sécurité Debian DSA-2131) ou d'utiliser un agent de messagerie alternatif comme Sendmail ou Postfix surtout si cet agent ne sert qu'à l'acheminement des messages du système. Il est également possible de s'affranchir du système de gestion de paquetages standard et recompiler une version plus récente d'Exim à partir des sources.

3 Zozzle, solution de détection de code JavaScript Malveillant

L'utilisation de *JavaScript* malveillants est encore et toujours l'un des vecteurs de compromissions les plus courants. Différentes voies sont explorées pour essayer de contrecarrer ces attaques, dont une présentée par des chercheurs de Microsoft, il y a quelques semaines, « la reconnaissance des codes malveillants par apprentissage ». Ce projet, nommé *Zozzle*, dérive en fait d'un autre un peu plus ancien, *Nozzle*. Ce dernier catégorise les codes comme malveillants ou sains en faisant une exécution partielle du code. Il a le désavantage de prendre trop de temps, ce qui le rend inutilisable en temps réel, au cours de la navigation. Il a donc été utilisé de façon asynchrone pour catégoriser un grand nombre de codes et définir des indicateurs. Ceux-ci servent ensuite à identifier un code source, de façon quasi statique, comme malveillant ou pas, en utilisant un algorithme basé sur le théorème de Bayes.

Cette nouvelle façon de faire, reposant sur une base de connaissances construite avec *Nozzle*, c'est *Zozzle*. La surcharge due à l'analyse avant l'exécution d'un code est annoncée comme minime par les chercheurs, ce qui permettrait d'intégrer une telle solution directement dans les navigateurs.

Il ne s'agit pour l'instant que d'une voie explorée par des chercheurs mais cela montre l'importance accordée à ces techniques d'attaque, et donc l'importance des risques associés.

Le CERTA recommande toujours la plus grande prudence avec l'utilisation du *JavaScript* et si possible de le limiter. De plus, il s'agit souvent que d'un moyen permettant l'exploitation d'une vulnérabilité d'un autre composant. Il est donc impératif de garder son système à jour. Respecter les bonnes pratiques reste donc, encore et toujours, la meilleure façon de se prémunir d'une majorité des possibles compromissions.

Documentation

- Page de présentation de Nozzle :
<http://research.microsoft.com/apps/pubs/default.aspx?id=76528>
- Page de présentation de Zozzle :
<http://research.microsoft.com/apps/pubs/default.aspx?id=141930>

4 LOIC, détournement malveillant de fonctionnalité

Cette semaine, de nombreux média se sont faits l'écho du logiciel *LOIC* (*Low Orbit Ion Canon*) qui est utilisé par des internautes prétendant venger l'arrestation du créateur du site *WikiLeaks*. *LOIC* est apparu en 2009 et n'a pas été conçu dans cette optique. Ce logiciel permet l'envoi massif de requêtes vers un serveur web déterminé. Ce logiciel peut être utilisé à des fins légitimes pour stresser un serveur web dans le cadre d'un test de monter en charge, par exemple. Dans le cadre des attaques de cette semaine, de nombreuses nouvelles variantes de ce logiciel sont apparues (mobile, écrite en *JavaScript*...) permettant l'envoi des ordres par une personne distante.

Le CERTA rappelle que le fait de prêter son aide sciemment (Art. 121-7 de Code Pénal) à la commission d'une infraction, en l'espèce d'une entrave au fonctionnement d'un système de traitement automatisé de données, est passible de 5 ans de prison et de 75 000 euros d'amende (Art. 321-2 du Code Pénal). De plus, ces nouvelles variantes une fois installées sur une machine peuvent laisser un accès distant et ainsi permettre à des personnes malveillantes de prendre le contrôle total de la machine.

Outre le caractère délictueux de l'utilisation, sans légitimité, de ce logiciel envers des serveurs distants, l'installation de ce type de logiciels peut porter atteinte à l'intégrité et à la confidentialité des données présentes sur le système hôte.

5 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/>

6 Rappel des avis émis

Dans la période du 03 au 09 décembre 2010, le CERTA a émis les avis suivants :

- CERTA-2010-AVI-574 : Multiples vulnérabilités dans les produits VMware
- CERTA-2010-AVI-575 : Vulnérabilités dans BIND
- CERTA-2010-AVI-577 : Vulnérabilité dans CUPS
- CERTA-2010-AVI-578 : Multiples vulnérabilités dans Google Chrome
- CERTA-2010-AVI-579 : Vulnérabilités dans AWStats
- CERTA-2010-AVI-580 : Vulnérabilité dans le module Safe de Perl
- CERTA-2010-AVI-581 : Multiples vulnérabilités dans QuickTime
- CERTA-2010-AVI-582 : Vulnérabilités dans WordPress
- CERTA-2010-AVI-583 : Multiples vulnérabilités dans VMware ESX
- CERTA-2010-AVI-584 : Vulnérabilité dans Citrix Web Interface

Durant la même période, les avis suivants ont été mis à jour :

- CERTA-2010-AVI-237-001 : Vulnérabilités dans OpenSSL (ajout de la référence au bulletin HP)

7 Actions suggérées

7.1 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 réglementaire, 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.

7.2 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.

7.3 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.

7.4 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.

7.5 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.

7.6 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 inexplicables 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.

7.7 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_rubrique67.html

8 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.

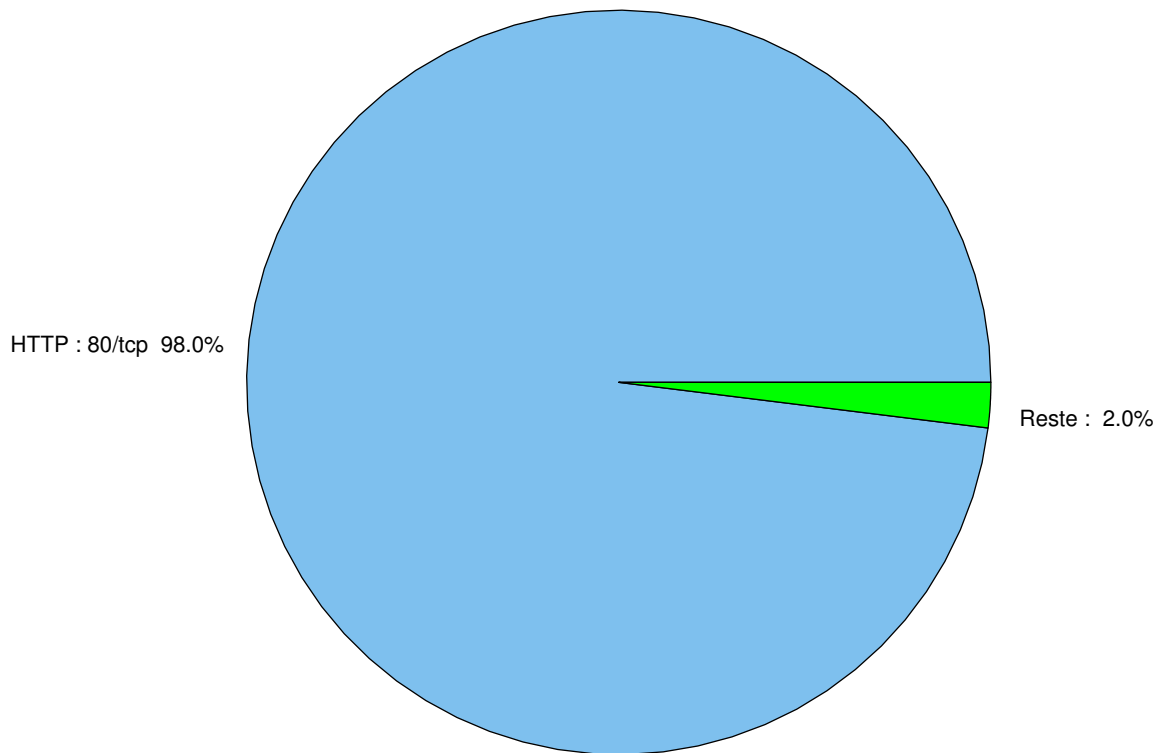


FIG. 1: Répartition relative des ports pour la semaine du 03 au 09 décembre 2010

port	pourcentage
80/tcp	98.47
25/tcp	0.85
1433/tcp	0.27
445/tcp	0.19
23/tcp	0.18
1080/tcp	0.15
22/tcp	0.07
135/tcp	0.06
3389/tcp	0.03
4899/tcp	0.02
3306/tcp	0.01

TAB. 2: Paquets rejetés

Liste des tableaux

1	Gestion du document	1
2	Paquets rejetés	6

Gestion détaillée du document

10 décembre 2010 version initiale.