Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 18 avril 2008
N° CERTA-2008-ACT-016

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2008-16

Gestion du document

Référence	CERTA-2008-ACT-016
Titre	Bulletin d'actualité 2008-16
Date de la première version	18 avril 2008
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-2008-ACT-016.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-2008-ACT-016/

1 Attaques sur GuppY

Le CERTA a traité cette semaine de nombreux cas de défigurations qui avaient tous en commun l'exploitation d'une vulnérabilité de *GuppY*. Cette vulnérabilité n'est pas nouvelle : elle est connue depuis janvier 2007, avait été mal corrigée par l'éditeur, puis avait été de nouveau corrigée en novembre 2007.

Ce qui est nouveau, c'est que les attaques sur *GuppY* affectaient autrefois des installations de versions 4.5.x. Or, depuis cette semaine, nous constatons de nombreuses intrusions sur des serveurs *GuppY* en version 4.6.3. Il est donc extrêmement important, pour les utilisateurs de *GuppY* en branche 4.6.x, de veiller à ce que les correctifs de sécurité aient été appliqués.

Le CERTA a mis à jour l'avis CERTA-2007-AVI-507 qui évoquait cette vulnérabilité, mais n'abordait pas le cas de la branche 4.6.x.

Documentation :

– Avis CERTA-2007-AVI-507 :
http://www.certa.ssi.gouv.fr/site/CERTA-2007-AVI-507/

– Site de GuppY :
http://www.freeguppy.org/

2 Sortie prochaine du Service Pack 3 de Windows XP

Le *Service Pack 3* de *Windows XP* est actuellement en *Release Candidate 2*. Certains sites sur l'Internet annoncent que la version finale devrait être téléchargeable pour les abonnés Technet et MSDN le 21 avril 2008. Le grand public, lui, devra attendre le 29 avril 2008 pour le télécharger. Enfin, ce *service pack* s'installerait automatiquement à partir du 10 juin 2008. Aucune annonce officielle de la part de Microsoft n'ayant cependant été faite, ces informations sont à prendre avec précaution.

Le *service pack 3* de *Windows XP* sera dans tous les cas moins important en nombre de correctifs et de nouvelles fonctionnalités que ne l'a été le *service pack 2*.

Il incluera tout d'abord toutes les mises à jour de *Windows XP* depuis le *service pack 2* (Août 2004) et des fonctionnalités qui étaient disponibles en téléchargement.

Comme nouvelles fonctionnalités, Microsoft indique les éléments suivants :

– le NAP (*Network Access Protection*), ce qui permet de mettre en quarantaine des machines non conformes à la politique de sécurité d'un réseau ;
– une nouvelle version du WPA (*Windows Product Activation*), permettant notamment d'installer *Windows XP SP3* sans clé de produit (comme pour *Windows Server 2003 SP2* et *Windows Vista*) ;
– une détection améliorée de routeurs pratiquant le *blackholing* (qui ignorent des paquets) ;
– *Microsoft Kernel Mode Cryptographic Module* (module de chiffrement noyau) ;
– davantage de descriptions dans les options de sécurité.

Enfin, l'éditeur a annoncé que *Internet Explorer 7* ne serait pas inclus dans le *service pack 3*.

2.1 Documentation

– Notes de changement pour Windows XP SP3 :
http://support.microsoft.com/kb/936929

3 Vulnérabilité dans le lecteur `Flash`

De nombreux articles récemment publiés font état d'une vulnérabilité dans le lecteur `Flash`. Cette vulnérabilité peut être exploitée par un fichier *SWF* spécialement conçu via un dépassement d'entier. Outre le véritable intérêt de l'étude qui a été publiée sur ce sujet et l'originalité de l'exploitation de cette vulnérabilité, le CERTA tient à faire certaines observations :

– Le lecteur `Flash`, par son aspect potentiellement omniprésent dans un système d'information, ne doit pas être pris à la légère dans sa gestion. En effet, le lecteur `Flash` peut être installé sur tout type de système d'exploitation et tout type de navigateur. Il peut donc être potentiellement installé sur presque toutes les machines d'un parc informatique ;
– lors du déploiement d'un parc informatique, il est important que l'administrateur se pose la question de la nécessité d'installer cette application sur les postes du réseau ;
– si l'application est installée, il est impératif d'en assurer un suivi rigoureux. Les animations et autres logiciels écrits avec le langage *ActionScript* sont très répandus sur l'Internet. La vulnérabilité en question est corrigée depuis le 08 avril 2008 par l'éditeur `Adobe`, et a fait l'objet de la publication de l'avis CERTA-2008-AVI-197. De plus, les techniques d'exploitation sont publiques.

Par ailleurs, `Flash` est un langage très riche en fonctionnalités. Depuis la version 9, il est possible d'implémenter de véritables « mini-serveurs » ou des robots (au sens *bot* du terme) dans des applications flash. En effet, les programmes en flash ont à leur disposition des fonctions permettant la mise en oeuvre de ressources réseau de type *socket*.

Un applicatif *flash* peut donc soit ouvrir des *socket* en écoute (comme un serveur) ou établir une connexion sur un serveur distant écoutant sur un port donné (comme un *bot*). Il est donc possible d'avoir un client réseau dans le contexte de la navigation, recevant ou émettant des paquets non maîtrisés vers une destination arbitraire. Ce comportement peut sembler assez proche de celui d'un cheval de Troie ou d'un *bot*.

Dans la mesure où l'on peut créer des `socket`, tout ou presque est envisageable : dialoguer avec les services réseau présents sur la machine ou sur le réseau local par exemple. Or, tout ce trafic sera vu comme provenant de la machine ! Il y a donc fort à parier que ces flux seront considérés comme légitimes.

Du point de vue de l'attaquant, cette technologie peut très bien être employée pour conduire une attaque de type déni de service sur le réseau local ou bien encore procéder à une collecte d'informations via des requêtes `DNS` ou `DHCP` spécifiques pour ensuite conduire une attaque. Il est d'ailleurs prévu par l'extension *flash* de procéder à des requêtes `DHCP` afin de déterminer s'il existe sur le réseau un mandataire *flash*...

Par conséquent, le CERTA recommande :

- de désactiver, par défaut, tous les scripts et codes exécutables via le navigateur ou les lecteurs multimedia afin de limiter l'exploitation de ce genre de vulnérabilités ;
- de n'installer que les applications et modules nécessaires ;
- de maintenir à jour l'ensemble des applicatifs du système d'information.

Documentation

- Avis CERTA-2008-AVI-197 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-197

4 Courriers électroniques de réponse non sollicités (*backscatter*)

4.1 Les faits

Plusieurs correspondants ont informé le CERTA ces dernières semaines d'une réception importante de courriers électroniques non sollicités sur leurs serveurs. Les courriels reçus ont les caractéristiques communes suivantes :

- il s'agit de messages notifiant un échec de remise ;
- ils sont visiblement émis par des serveurs de messagerie. L'adresse émettrice est de la forme `postmaster`, `MAILER-DAEMON`, etc. Le champ de retour `Return-Path:` est vide.
- le sujet est un message d'erreur de type :
  - « Notification d'état de remise (Echec) » ;
  - « NOTICE: mail delivery status » ;
  - « Undeliverable mail: *sujet initial* » ;
  - « Undeliverable Mail » ;
  - « Undeliverable: *sujet initial* » ;
  - « Returned mail: see the transcript[FAILED(1)] » ;
  - « Delivery Notification: Delivery has failed » ;
  - etc.
- le corps du message contient un message d'erreur justifiant l'impossibilité de remettre le courriel, par exemple en signalant qu'un ou plusieurs destinataires n'existent pas.
- le corps du message peut contenir une copie d'un autre message, avec un en-tête bien différent, et avec le champ `From:` faisant apparaître le destinataire du message d'échec de remise ;
- des pièces jointes peuvent également s'ajouter aux données précédentes.

En voici un exemple :

```
Subject: Undelivered Mail
From: <MAILER-DAEMON@domainC>
Date: Fri, 18 Apr 2008 14:19:42 +0200
To: <monsieurB@domainB>
X-Account-Key: account2
Return-Path: <>
X-Original-To: monsieurB@domainB
Delivered-To: monsieurB@domainB
Received: from serveurMail@domainC by serveurMail@domainB (Postfix)
            with ESMTP id XXXXXXXX
            for <monsieurB@domainB>; Fri, 18 Apr 2008 14:10:52 +0200
Received: ....
(...)
```

```
Your message to the following recipients cannot be delivered:

<toto1@domainC>
#550 5.1.1
The recipient's e-mail address was not found in the recipient's e-mail system.

(...)
```

L'en-tête globale du courriel semble dans la majorité des cas légitime. Il ne semble pas « forgé ».

4.2 Le problème

Ces courriels sont les « résidus » de messages envoyés avec une adresse émettrice usurpée et ayant provoqué un message de retour. La cause de celui-ci peut être :

- l'utilisateur n'existe pas ;
- l'utilisateur a sa boîte de message électronique qui a atteint sa taille maximale autorisée ;
- l'utilisateur est en congé, et il s'agit d'une réponse automatique ;
- le message est refusé car déclaré dangereux (code malveillant ou format de fichier filtré...).

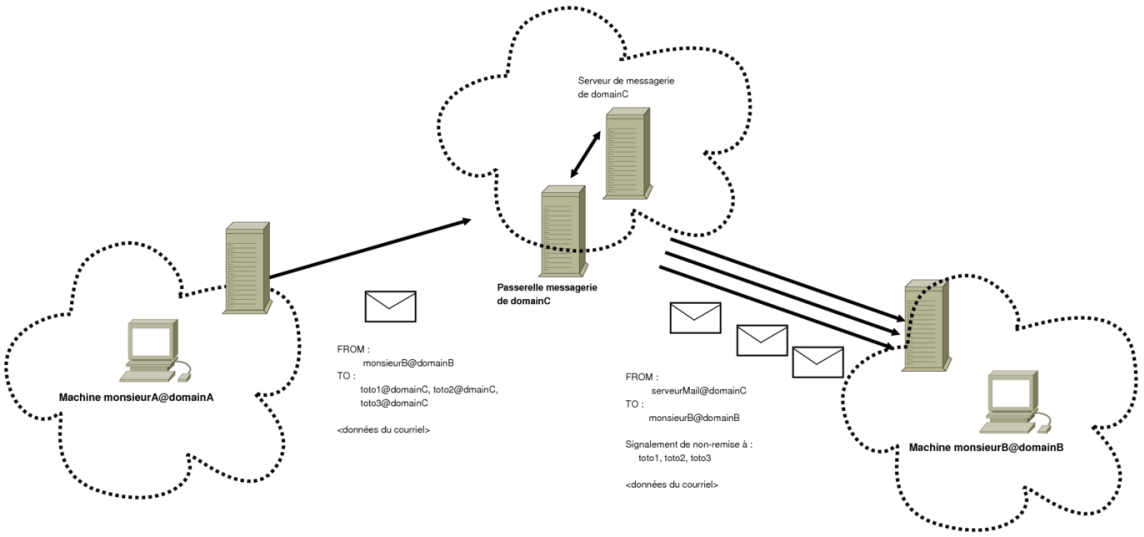

FIG. 1: Schéma présentant un scénario de production de "*backscatter*"

Le terme *backscatter* (« rétrodiffusion » en français) a été utilisé récemment pour caractériser ce comportement. Il est cependant trompeur, car il peut également être associé à des usurpations d'adresses IP : dans le cas d'attaques par inondation de trames TCP SYN usurpant de multiples adresses IP sources, les *backscatters* sont les retours TCP non sollicités vers ces adresses par la machine victime.

- Analyses d'attaques par déni-de-service en s'appuyant sur les traces de type *backscatter* :
  http://www.caida.org/data/publications/bydataset/index.xml#backscatter

Certains parlent donc de "*e-mail backscatters*". Cela peut se définir comme des messages de réponse non sollicités.

Il s'agit donc initialement bien d'une usurpation d'adresse électronique. Cependant le second souci provient du comportement très hétérogène des serveurs de messagerie.

Dans le meilleur des cas concernant la figure 1, c'est le serveur émetteur de monsieurB qui devrait retourner un rapport de non remise après avoir obtenu une erreur `550 no such user` du serveur de domainC.

Cependant le serveur de domainC ne traite pas toujours directement la réception (usage de passerelles). Sur le schéma précédent, le serveur de domainC va générer des messages d'erreurs qui seront retransmis par la passerelle de messagerie.

Par ailleurs, le comportement peut varier si le message d'origine contient plusieurs destinataires. Pour un message envoyé avec une adresse usurpée, cette dernière peut recevoir autant de messages d'erreurs que de destinataires erronés. Ce comportement n'est pas souhaité par le standard RFC 2821 mais est mis en oeuvre par certains serveurs.

Le standard est flou concernant le contenu du message d'erreur : celui-ci doit permettre d'identifier le message d'origine, mais il n'est pas nécessaire de copier tout le corps au format texte ni les pièces jointes.

4.3 Les motivations

Des personnes malveillantes peuvent être amenées à utiliser les propriétés précédentes pour différentes raisons:

- cibler le serveur de domainC : le lecteur aura compris que pour un courriel envoyé, cela peut générer le traitement de celui-ci et l'émission d'une ou plusieurs réponses. Cela peut provoquer un gêne du service de messagerie, mais aussi au niveau de la bande passante générale, si les pièces jointes sont effectivement recopiées dans les messages d'erreur. Cet envoi indirect permet d'amplifier le trafic ;
- déterminer les adresses fonctionnelles du domainC. Seules celles ne provoquant pas d'erreurs récupérées par ailleurs sont acceptées par le serveur. Dans ce cas, la personne malveillante contrôle la machine émettrice (celle de monsieurA), ainsi que celle de réception (celle de monsieur B) ;
- atteindre indirectement monsieurB pour :
  - lui faire parvenir du *spam* indirectement. Ce dernier semble émis de domainC. Le spam peut contenir des liens vers des sites de filoutage ou vers des pages Web au contenu dangereux pour le navigateur ;
  - lui remplir sa boîte à lettres jusqu'à saturation. Les filtrages ne sont pas simples, car les sources émettrices peuvent être très différentes (les serveurs manipulés comme domainC) , et la solution consistant à filtrer tout message d'erreur peut être mal perçu par les utilisateurs. Ces derniers n'ont plus de réel moyen pour savoir si leur courriel est envoyé à la bonne adresse, l'accusé de réception étant émis au bon-vouloir du destinataire.

4.4 Que faire en cas de réception importante de courriels ?

Il n'existe pas de solution absolue. Les messages d'erreurs sont d'une certaine manière légitimes et intrinsèques au fonctionnement de SMTP. Ils peuvent cependant se manifester par un volume anormal de messages que le serveur a du mal à gérer correctement. C'est un déni de service.

Parmi les solutions envisageables, il y a :

- la mise en place d'une passerelle en amont gérant un premier filtrage, afin de délester la tâche du serveur ;
- le mise en place de serveurs MX supplémentaires en cas d'indisponibilité temporaire de l'un d'eux ;
- la définition au niveau réseau d'une liste « blanche » ou de confiance des serveurs courants. Une priorité plus importante peut être éventuellement donnée aux communications avec ceux-ci.
- la mise en place de limitations ou quotas de connexions, au niveau du pare-feu ou du service de messagerie ;
- le filtrage de certains champs d'en-tête par le serveur de messagerie, quand cette fonctionnalité est offerte. Attention! Cela peut aussi avoir des impacts sur des messages légitimes. Par exemple, il est possible dans Postfix de personnaliser le fichier `/etc/postfix/header_checks` :

```
/^Content-Type: multipart\/report; report-type=delivery-status\;/ REJECT
                                                        no third-party DSNs
/^Content-Type: message\/delivery-status; / REJECT no third-party DSNs
```

Il est également possible de filtrer certaines adresses. Sous Postfix, une solution consiste à ajouter une liste dans `smtpd_recipient_restrictions` et/ou `smtpd_sender_restrictions` :

```
Ajout d'une ligne comme :
check_sender_access hash:/chemin_Postfix/maps/access_sender

Et dans le fichier /chemin_Postfix/maps/access_sender :
serveurMail@domainC REJECT

Puis lancer la commande :
postmap access_sender
```

- le filtrage vérifiant la légitimité des utilisateurs émetteurs (aussi appelé `SAV` pour *Sender Address Verification* ou *callback*). Cette technique est supportée par `Exim` et `Postfix`. Elle consiste à contrôler l'adresse de retour. Néanmoins son impact reste limité compte-tenu de la construction des courriels actuels qui tendent à sutiliser systématiquement des adresses émettrices existantes ;
- utiliser des propriétés dédiées aux applications déployées. Ainsi, il existe pour l'outil SpamAssassin des outils pour définir des règles dédiées : `VBounceRuleset`.
- surveiller les journaux de messagerie, en s'aidant si besoin d'utilitaires comme logparser (pour les journaux Exchange) ou maillogconverter.pl du projet awstats (pour les journaux Postfix, sendmail ou qmail). Les commandes en ligne classiques (`cut`, `sort`, `cat`, `sed`, etc.) sont aussi très pratiques pour analyser des points particuliers dans les journaux

4.5 Documentation

- Site du projet awstats, page de configuration pour les journaux de messagerie : http://awstats.sourceforge.net/docs/awstats_faq.html#MAIL
- RFC 2821, "Simple Mail Transfer Protocol", avril 2001 : http://www.ietf.org/rfc/rfc2821.txt
- RFC 3464, "An Extensible Message Format for Delivery Status Notifications", janvier 2003 : http://www.ietf.org/rfc/rfc3464.txt
- RFC 821, "Simple Mail Transfer Protocol", août 1982 : http://www.ietf.org/rfc/rfc821.txt
- Note d'information, "Postfix Address Verification Howto" : http://www.postfix.org/ADDRESS_VERIFICATION_README.html
- Notes concernant `VBounceRuleset` pour SpamAssassin : http://wiki.apache.org/spamassassin/VBounceRuleset
- S. Frei, I. Silvestri, G. Ollmann, "Mail Non-Delivery Message DDoS Attacks", 2004 : http://www.techzoom.net/publications/mail-non-delivery-attack/index.en

5 Attaques Massives de type *SQL Injection* - Suite

5.1 Suite de l'histoire

En mars, le CERTA avait abordé le sujet de nombreux sites défigurés (bulletin d'actualité CERTA-2008-ACT-012). L'analyse des traces avait conduit à penser qu'il s'agissait d'une injection MsSQL/ASP, et le grand nombre de sites touchés laissait pressentir une recherche et une exploitation automatique des vulnérabilités. Un code au fonctionnement correspondant et laissant des traces similaires a finalement été trouvé.

Le script ajoute par défaut un cadre (*iframe*) pointant vers un code malveillant à toutes les pages défigurées, ce qui était une des traces significatives. L'adresse hébergeant le code malveillant se trouve à l'étranger mais ne répond plus.

- Le script se connecte à *Google* et recherche des sites vulnérables à l'aide de la requête par défaut *inurl:".asp" inurl:"a="*. Cette requête est configurable.
- Il tente d'injecter une requête SQL sur les sites retournés par la recherche. La requête en question cherche dans toutes les tables utilisateurs (*sysobjects.xtype='U'*) les colonnes de type « text » (*syscolumns.xtype : 99(ntext) 35(text) 231(nvarchar) 167(varchar)*) pour injecter dans chaque ligne le code malveillant.
- Avant de se lancer, le script essaie de se connecter au script *pay.asp*, situé également à l'étranger, avec l'argument *SN*. On imagine que son utilisation est payante et qu'il s'agit de quelque chose comme une vérification de numéro de licence.

5.2 Les recommandations

- Pour les développeurs :
  - mettre en place des contrôles des variables dans les pages ASP.
- Pour les administreurs :
  - contrôler les flux ;
  - surveiller les traces dans le journaux ;

  - éviter de lancer les applications web avec un utilisateurs aux droits élevés ;
  - verifier l'intégrité des bases de données.
- Pour les utilisateurs :
  - mettre à jour vos applications, le code malveillant exploite des vulnérabilités corrigées ;
  - limiter l'utilisation du *JavaScript*, le code malveillant ne peut pas s'exécuter sans ;
  - éviter de naviguer avec un utilisateurs aux droits élevés.

5.3 Documentation

- Bloc-notes du SANS du 16 avril 2008 :
  http://isc.sans.org/diary.html?storyid=4294
- Bulletin d'actualités du CERTA du 21 mars 2008 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-012/index.html

6 Ports observés

Le tableau 3 et la figure 2 montrent les rejets pour les ports sous surveillance que nous avons constatés sur des dispositifs de filtrage, entre le 10 et le 17 avril 2008.

7 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=1935
- 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/

8 Rappel des avis émis

Dans la période du 11 au 17 avril 2008, le CERTA a émis les avis suivants :

- CERTA-2008-AVI-198 : Vulnérabilités dans Symantec Mail Security
- CERTA-2008-AVI-199 : Multiples vulnérabilités d'IBM Lotus Notes
- CERTA-2008-AVI-200 : Vulnérabilité du logiciel Adobe ColdFusion

– CERTA-2008-AVI-201 : Vulnérabilités dans Drupal
– CERTA-2008-AVI-202 : Vulnérabilité dans HP Storage Essentials
– CERTA-2008-AVI-203 : Vulnérabilité dans rsync
– CERTA-2008-AVI-204 : Vulnérabilités dans IBM HTTP Server
– CERTA-2008-AVI-205 : Vulnérabilité dans Symantec Altiris Deployment Solution
– CERTA-2008-AVI-206 : Multiples vulnérabilités dans ClamAV
– CERTA-2008-AVI-207 : Multiples vulnérabilités dans VMware ESX Server
– CERTA-2008-AVI-208 : Multiples vulnérabilités dans les produits Oracle
– CERTA-2008-AVI-209 : Vulnérabilité de Firefox
– CERTA-2008-AVI-210 : Vulnérabilité dans Cisco NAC Appliance
– CERTA-2008-AVI-211 : Multiples vulnérabilités dans Apple Safari
– CERTA-2008-AVI-212 : Vulnérabilité dans divers produits Computer Associates
– CERTA-2008-AVI-213 : Vulnérabilités dans IBM DB2
– CERTA-2008-AVI-214 : Multiples vulnérabilités dans HP Openview

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

– CERTA-2007-AVI-507-001 : Vulnérabilité dans GuppY (prise en compte de la branche 46)
– CERTA-2008-AVI-208-001 : Multiples vulnérabilités dans les produits Oracle (ajout de références CVE associés à cette mise à jour)

9 Actions suggérées

9.1 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.

9.2 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.

9.3 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.

9.4 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.

9.5 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.

9.6 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.

9.7 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, la DCSSI dispose d'un centre de formation :

http://www.formation.ssi.gouv.fr

10 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.

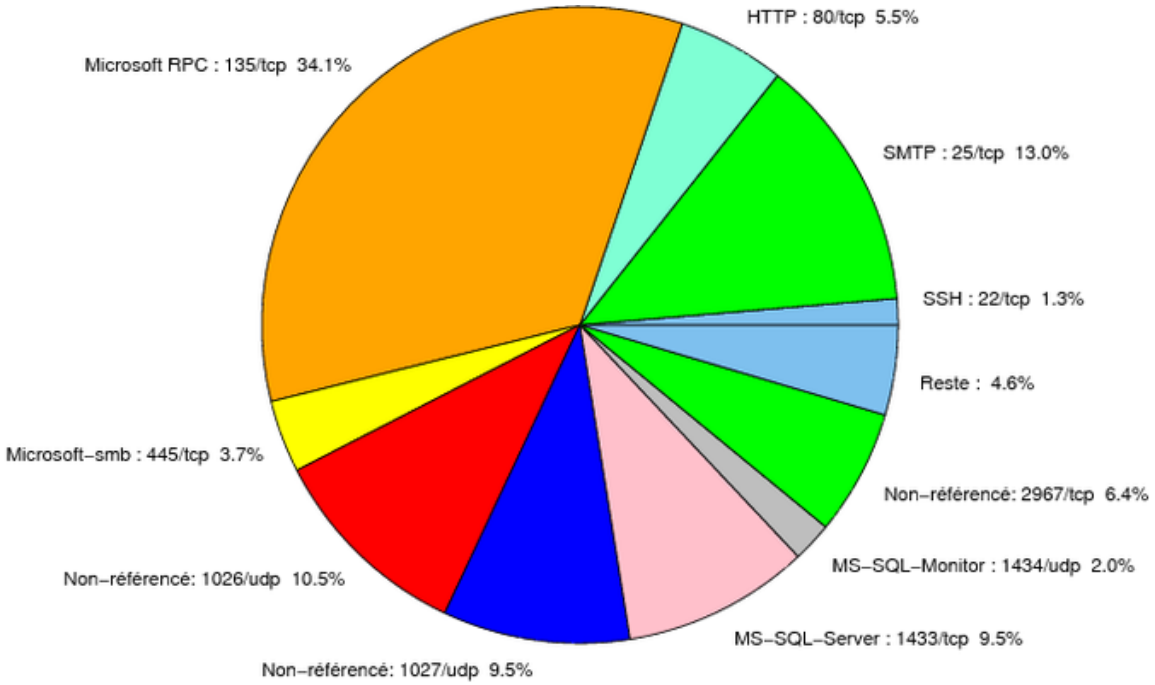

FIG. 2: Répartition relative des ports pour la semaine du 10.04.2008 au 17.04.2008

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
22	TCP	SSH	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
23	TCP	Telnet	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER CERTA-2007-ALE-005-001
25	TCP	SMTP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
42	TCP	WINS	–	http://www.certa.ssi.gouv.fr/site/CER
69	UDP	IBM Tivoli Provisioning Manager	–	http://www.certa.ssi.gouv.fr/site/CER
80	TCP	HTTP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
106	TCP	MailSite Email Server	–	– http://www.certa.ssi.gouv.fr/site/CER
111	TCP	Sunrpc-portmapper	–	http://www.certa.ssi.gouv.fr/site/CER
119	TCP	NNTP	–	http://www.certa.ssi.gouv.fr/site/CER
135	TCP	Microsoft RPC	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
137	UDP	NetBios-ns	–	http://www.certa.ssi.gouv.fr/site/CER
139	TCP	NetBios-ssn et samba	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER

				http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
143	TCP	IMAP	–	http://www.certa.ssi.gouv.fr/site/CER
389	TCP	LDAP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
427	TCP	Novell Client	–	http://www.certa.ssi.gouv.fr/site/CER
443	TCP	HTTPS	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
445	TCP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
445	UDP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CER
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	http://www.certa.ssi.gouv.fr/site/CER
1433	TCP	MS-SQL-Server	–	http://www.certa.ssi.gouv.fr/site/CER
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CER
2100	TCP	Oracle XDB FTP	–	http://www.certa.ssi.gouv.fr/site/CER
2381	TCP	HP System Management	–	http://www.certa.ssi.gouv.fr/site/CER
2512	TCP	Citrix MetaFrame	–	http://www.certa.ssi.gouv.fr/site/CER
2513	TCP	Citrix MetaFrame	–	http://www.certa.ssi.gouv.fr/site/CER
2745	TCP	–	Bagle	–
2967	TCP	Symantec Antivirus	Yellow Worm	http://www.certa.ssi.gouv.fr/site/CER
3104	TCP	CA Message Queuing	–	http://www.certa.ssi.gouv.fr/site/CER
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
3268	TCP	Microsoft Active Directory	–	http://www.certa.ssi.gouv.fr/site/CER
3306	TCP	MySQL	–	–
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
5151	UDP	IPSwitch WS_TP	–	http://www.certa.ssi.gouv.fr/site/CER
5151	TCP	ESRI ArcSDE	–	http://www.certa.ssi.gouv.fr/site/CER
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER

6014	TCP	IBM Tivoli Monitoring	–	http://www.certa.ssi.gouv.fr/site/CER
6070	TCP	BrightStor ARCserve/Enterprise Backup	–	http://www.certa.ssi.gouv.fr/site/CER
6101	TCP	Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CER
6106	TCP	Symantec Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CER
6129	TCP	Dameware Miniremote	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
6502	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CER
6503	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CER
6504	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CER
8080	TCP	IBM Tivoli Provisioning Manager	–	http://www.certa.ssi.gouv.fr/site/CER
8866	TCP	–	Porte dérobée Bagle.B	–
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
10080	TCP	Amanda	MyDoom	–
10110	TCP	IBM Tivoli Monitoring	–	http://www.certa.ssi.gouv.fr/site/CER
10916	TCP	Ingres	–	CERTA-2007-AVI-275-001
10925	TCP	Ingres	–	CERTA-2007-AVI-275-001
12168	TCP	CA eTrust antivirus	–	http://www.certa.ssi.gouv.fr/site/CER
13701	TCP	Veritas NetBackup	–	http://www.certa.ssi.gouv.fr/site/CER
18264	TCP	CheckPoint interface	–	http://www.certa.ssi.gouv.fr/site/CER
54345	TCP	HP Mercury	–	http://www.certa.ssi.gouv.fr/site/CER
65535	UDP	LANDesk Management Suite	–	http://www.certa.ssi.gouv.fr/site/CER

TAB. 2: Correctifs correspondant aux ports destination des paquets rejetés

port	pourcentage
135/tcp	34.11
25/tcp	13
1026/udp	10.46
1433/tcp	9.5
2967/tcp	6.37
80/tcp	5.45
445/tcp	3.68
1434/udp	2.02
22/tcp	1.32
3306/tcp	0.95
137/udp	0.73
23/tcp	0.66
143/tcp	0.58
4899/tcp	0.4
139/tcp	0.29
1080/tcp	0.25
3127/tcp	0.22
10080/tcp	0.07
42/tcp	0.03

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

18 avril 2008 version initiale.