Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 février 2009
N° CERTA-2009-ACT-007

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2009-07

Gestion du document

Référence	CERTA-2009-ACT-007
Titre	Bulletin d'actualité 2009-07
Date de la première version	13 février 2009
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-2009-ACT-007.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-2009-ACT-007/

1 Appliquer les correctifs, mais pas seulement

1.1 Fenêtre de vulnérabilité

La littérature utilise la notion de fenêtre de vulnérabilité pour désigner l'intervalle de temps entre la publication d'une vulnérabilité et l'application des mesures par l'administrateur d'un système d'information. Dans sa généralité, ce concept est intéressant, mais sa traduction naïve peut laisser persister des vulnérabilités.

La publication de la vulnérabilité peut revêtir la forme d'une publication de l'éditeur d'un logiciel ou d'une société spécialisée en SSI. Elle peut également se traduire par la publication d'un code d'exploitation de la vulnérabilité.

Dans les deux cas, cette publication peut précéder ou être postérieure à la mise à disposition d'un correctif par l'éditeur. Cette mise à disposition est souvent la publication implicite de la vulnérabilité. En analysant le correctif ou la documentation associée, la vulnérabilité est identifiable.

L'administrateur peut se contenter d'appliquer le correctif de l'éditeur pour renforcer son système. Si cette pratique est nécessaire, elle peut se révéler insuffisante.

1.2 Limite du concept

La course entre les attaquants et les administrateurs est « sans pitié ». En particulier, des codes d'exploitation peuvent être disponibles sur l'internet moins de 24 heures après la publication du correctif. Un système peut avoir été compromis avant que l'administrateur ait eu le temps d'appliquer les correctifs. Ce dernier peut être tributaire de moyens de récupération du correctif, de procédures internes de test, d'information des clients...

La mise à jour du système compromis peut donc laisser le système vulnérable, sans que l'administrateur en ait conscience.

Un premier exemple simple concerne une vulnérabilité qui permet l'accès à un fichier de mots de passe d'administration protégé par un chiffrement faible. Le code d'exploitation de la vulnérabilité permet à un agresseur de récupérer ledit fichier. Pendant que l'administrateur applique le correctif, l'agresseur, sur son propre système « casse » le chiffrement et récupère les mots de passe. Alors que l'administrateur croit son système redevenu sûr, celui-ci est compromis par utilisation du compte d'administration.

Un deuxième exemple concerne la création d'éléments secrets (clefs, mots de passe). Dans la version vulnérable du système, ces éléments sont faibles, prédictibles ou insuffisament variés. Le correctif de l'éditeur vise à modifier le générateur pour durcir les éléments secrets qui seront créés dans le futur. Pour les éléments déjà créés et faibles, l'éditeur peut tout au plus créer des outils pour les détecter. Il est nécessaire que ces éléments soient remplacés par l'administrateur ou les utilisateurs du système. Il en est de même de leurs dérivés dont la fiablité n'est plus assurée, comme des signatures produites avec des clefs faibles.

1.3 Recommendations

Lorsqu'une vulnérabilité est publique et qu'un correctif est disponible, il est sage :

- de vérifier que le système n'a pas déjà été compromis, par exemple en analysant les journaux de connexions ;
- de le nettoyer le cas échéant ;
- bien entendu, d'appliquer les correctifs sur le système (redevenu) sain ;
- d'appliquer les mesures d'accompagnement sur les données, comme regénérer des clefs ou changer des mots de passe. En particulier, toute vulnérabilité permettant à un utilisateur malveillant de lire des informations sensibles donc être regardée sous cet angle. Les éditeurs signalent généralement ces mesures dans leurs bulletins de sécurité.

1.4 Documentation

- Avis du CERTA *Vulnérabilité dans la version OpenSSL de Debian* du 13 mai 2008 : http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-239/
- Avis du CERTA *Vulnérabilité dans OpenSSH pour Debian et Ubuntu* du 15 mai 2008 : http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-246/
- Logiciel Debian de détection des clés faibles : http://security.debian.org/project/extra/dowkd/dowkd.pl.gz
- Avis du CERTA *Multiples vulnérabilités de TYPO3* du 21 janvier 2009 : http://www.certa.ssi.gouv.fr/site/CERTA-2009-AVI-024/
- Avis du CERTA *Vulnérabilité de TYPO3* du 11 février 2009 : http://www.certa.ssi.gouv.fr/site/CERTA-2009-AVI-063/

2 Waledac vous souhaite une joyeuse Saint-Valentin

Dans le bulletin d'actualité CERTA-2009-ACT-003 du 16 janvier 2009, nous vous informions de l'émergence d'une nouvelle famille de vers se propageant entre autres par courriel, et ayant à peu près les mêmes fonctionnalités que Storm Worm : la famille appelée Waledac.

Depuis, chaque événement particulier repris dans la presse semble provoquer une nouvelle variante de ce ver. Ce fut le cas lors de l'intronisation du nouveau président des Etats-Unis. C'est encore le cas ces dernier temps à l'occasion de la fête des amoureux. Les courriels envoyés contiennent un message en rapport avec l'amour, et incitent l'utilisateur à aller visiter une page. Sur cette page, plusieurs cœurs sont affichés et un message (comme *"Guess which one is for you"*) incite l'utilisateur à cliquer sur un des cœurs. Ceci a pour effet de proposer en téléchargement le virus qui sera ensuite exécuté et installé par l'utilisateur.

Même si le mécanisme d'infection semble très naïf, il reste encore très efficace et fonctionnel. Nous vous rappelons donc de ne pas cliquer sur des mails douteux, de surfer autant que possible avec un compte disposant de droits limités, et de bien réfléchir avant d'installer tout logiciel inconnu.

Si malgré tout vous pensez avoir été infectés, nous vous invitons à vous référer au bulletin d'actualité CERTA-2009-ACT-003 du 16 janvier 2009 afin de découvrir certaines contremesures.

3 Vulnérabilité dans l'autorun sur Windows

3.1 Rappel sur l'autorun

L'autorun est un mécanisme des systèmes d'exploitation Windows permettant notamment de définir des actions lors de certaines interactions d'un utilisateur avec des périphériques de stockage. Sont concernés, par exemple, les clés USB, disques durs et disques montés en réseau.

Ces actions sont définies dans un fichier `autorun.inf`, qui doit se trouver à la racine du lecteur (volume). Ce fichier permet de définir d'autres paramètres, comme l'icône et le label sous lesquels le volume sera présenté.

Voici des exemples d'actions paramétrables au moyen de ce fichier :

- programme à exécuter automatiquement lors de l'insertion du média (CDrom, clés U3) ;
- programme à exécuter par défaut (« double-clic » sur l'icône) ;
- programme à exécuter lorsque l'utilisateur choisit « Explorer » dans le menu contextuel du périphérique ;
- programme à exécuter lorsque l'utilisateur choisit « Ouvrir » dans le menu contextuel du périphérique.

Le lecteur aura vite compris qu'il est difficile d'accéder à un périphérique de stockage ainsi configuré sans faire appel à une action définie dans le fichier `autorun.inf`. Cela reste toutefois possible, par exemple, en naviguant via l'interpréteur de commandes `cmd.exe`.

De nombreux codes malveillants utilisent ce fichier `autorun.inf` pour infecter des ordinateurs par clé USB. Il est donc vivement recommandé de désactiver cette fonctionnalité.

3.2 Détails sur le fonctionnement de l'autorun

L'autorun fonctionne selon le principe suivant. Lorsqu'un nouveau média est détecté (insertion d'une clé USB, par exemple), le système crée une clé de registre au format suivant :
`HKCU/Software/Microsoft/Windows/CurrentVersion/Explorer/MountPoints2/<ID>`,
`<ID>` représentant un identifiant unique pour le média.

En fonction du fichier `autorun.inf` détecté, cette clé sera peuplée de sous-clés décrivant les programmes à exécuter. Ainsi, si dans le fichier `autorun.inf` on met la ligne suivante :

```
[autorun]
shell\open\command=calc.exe
```

alors la clé suivante sera créée :
`HKCU/Software/Microsoft/Windows/CurrentVersion/Explorer/MountPoints2/<ID>/Shell/open/command`
avec une valeur par défaut qui sera `calc.exe`.

Lorsque ces clés sont supprimées, l'autorun ne fonctionne pas tant que le média n'est pas réinséré, ou que l'ordinateur est redémarré avec le média connecté.

La clé `HKCU/Software/Microsoft/Windows/CurrentVersion/Explorer/MountPoints2/<ID>`
n'est jamais supprimée par le système. Les sous-clés, décrivant les paramètres décrits dans le fichier `autorun.inf` peuvent toutefois être supprimées dans certains cas. Voici les cas observés :

- lorsqu'un média est inséré, les sous-clés qui existent pour ce média sont supprimées puis recréées (donc écrasées) ;
- lorsqu'un ordinateur est démarré avec le média inséré, les sous-clés sont supprimées ;
- lorsque l'explorateur énumère les médias (ouverture du poste de travail, par exemple) pour la première fois, les sous-clés sont peuplées.

Ainsi, en règle générale, `MountPoints2` contient tous les médias insérés dans l'ordinateur et les paramètres d'autorun détectés. Ceci en fonction de l'utilisateur connecté, car c'est une clé dans la ruche `HKEY_USERS`.

3.3 Désactivation de l'autorun

La méthode donnée par Microsoft pour désactiver l'autorun est l'édition de la valeur `NoDriveTypeAutorun` dans la clé suivante :
`HKLM/Software/Microsoft/Windows/CurrentVersion/Policies/Explorer`
(ou `HKCU` pour se limiter à l'utilisateur, et non la machine entière)

Il est parfois nécessaire de la créer car cette clé n'est pas présente par défaut. La valeur affectée à `NoDriveTypeAutorun` va définir quels types de lecteurs ne doivent pas utiliser la fonctionnalité d'autorun. Pour le désactiver sur tous les types de disque, il faut mettre la valeur `0xFF` (pour plus de détails, se référer à la note d'information CERTA-2006-INF-006).

L'autorun peut également être désactivé en éditant les stratégies de groupe pour la machine ou pour l'utilisateur (`gpedit.msc`). Les mêmes clés de registre sont modifiées automatiquement par le système. Le paramètre se trouve dans :

```
Configuration ordinateur (ou utilisateur)
                -> Modèles d'administration
                -> Système
                -> Désactiver le lecteur automatique
```

3.4 La vulnérabilité

La vulnérabilité décrite dans l'avis CERTA-2009-AVI-064 concerne justement le moyen de protection décrit ci-dessus, qui ne fonctionne pas correctement sans l'application d'un correctif développé par Microsoft. Ainsi, même si la valeur `0xFF` est utilisée pour `NoDriveTypeAutorun`, il est possible d'exécuter du code arbitraire lorsqu'un utilisateur interagit avec le média.

Dans les cas observés par le CERTA, la clé `NoDriveTypeAutorun` n'était en effet que consultée par `explorer.exe` lors de l'énumération des médias par celui-ci (ouverture du poste de travail, par exemple). Dans ce cas précis uniquement, les sous-clés de chaque média, qui étaient supprimées par le démarrage de l'ordinateur, n'étaient donc pas repeuplées. En revanche, lorsqu'un média était inséré, `explorer.exe` ne consultait pas la clé `NoDriveTypeAutorun` et remplissait les sous-clés, ce qui causait donc l'exécution des programmes définis dans les fichiers `autorun.inf`.

Ainsi, sur un système vulnérable, la seule protection apportée par la désactivation de l'autorun était que ce dernier n'était effectivement désactivé que pour les médias déjà insérés lors du démarrage de Windows! Mais cette protection ne fonctionnait pas pour les médias insérés après démarrage...

Ce problème concerne toutes les versions de Windows. Le correctif en question n'est cependant pas proposé dans les mises à jour automatiques pour toutes les versions de Windows.

Ainsi, pour Windows Vista et Windows Server 2008, la mise à jour était incluse dans le bulletin MS08-038 (kb950582), portant sur la fonction de recherche de l'explorateur de fichiers (CVE-2008-1435). En lisant avec détail le bulletin de sécurité de Microsoft, il est indiqué en effet dans la partie « Forum aux questions » que la mise à jour contient une autre modification qui « désactive correctement le clic-droit et le double-clic contrôlés par la clé de registre NoDriveTypeAutorun » (CVE-2008-0951). Ceci probablement car le fichier incriminé est le même pour les deux vulnérabilités.

Les systèmes Windows 2000, Windows XP et Windows Server 2003 n'étant pas affectés par la vulnérabilité principale de MS08-038, n'ont pas bénéficié de cette mise à jour automatique. Toutefois, comme cela est indiqué dans le bulletin kb953252, il est possible de télécharger le correctif pour l'autorun manuellement, et ce depuis août 2008.

On remarquera que le correctif ne change pas l'utilisation de la clé `MountPoints2`. Celle-ci est toujours peuplée lors de l'insertion d'un média. On observe en effet que Windows effectue un traitement du fichier `autorun.inf`. Une nouvelle valeur est cependant ajoutée, qui « contrôle » la clé `NoDriveTypeAutorun`. Ces deux clés sont consultées après traitement du fichier `autorun.inf`. Cette nouvelle valeur est la suivante :
`HKLM/Software/Microsoft/Windows/CurrentVersion/Policies/Explorer/HonorAutorunSetting`.

Ceci signifie en français « respecter le paramètre d'autorun ». Si cette valeur est à 1 (valeur par défaut), alors la désactivation via la clé `NoDriveTypeAutorun` sera enfin effective! Si la valeur est à 0, l'autorun sera totalement activé (et non partiellement, comme cela était le cas sur les machines vulnérables).

3.5 Un autre moyen pour désactiver l'autorun

Le CERTA recommande évidemment d'appliquer le correctif de Microsoft dès que possible, et d'utiliser la stratégie de groupe ou de modifier directement la base de registre pour mettre la valeur `0xFF` à

NoDriveTypeAutorun.

Toutefois, il faut savoir qu'il existe un autre moyen de désactiver l'autorun. Il consiste à désactiver définitivement l'utilisation des fichiers autorun.inf.

Cela se fait en ajoutant la clé suivante :

HKLM/Software/Microsoft/Windows NT/CurrentVersion/IniFileMapping/autorun.inf

et en lui affectant comme valeur par défaut @SYS:DoesNotExist.

Dans ce cas, le fichier autorun.inf n'est pas du tout traité par Windows. En effet, la clé IniFileMapping consiste à indiquer à Windows quels fichiers ini (utilisés par les programmes avant la base de registre) doivent être ignorés et quelle clé de registre doit être consultée à la place. Ici, on indique à Windows de ne pas traiter les valeurs contenues dans autorun.inf et d'utiliser plutôt la clé HKLM/Software/DoesNotExist, qui n'existe évidemment pas.

On remarquera, après utilisation de ce contournement, que les sous-clés de MountPoints2/<ID> ne sont effectivement pas créées et que le fichier autorun.inf n'est pas traité par Windows. Attention toutefois aux effets de bord non maîtrisés qui pourraient survenir.

3.6 Documentation

- Avis du CERTA CERTA-2009-AVI-064 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2009-AVI-064/
- Bulletin Microsoft KB953252 :
  http://support.microsoft.com/kb/953252/fr
- Note d'information CERTA-2006-INF-006 « Risques associés aux clés USB » :
  http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-006/
- Alerte de l'US CERT TA09-020A du 20 janvier 2009 :
  http://www.us-cert.gov/cas/techalerts/TA09-020A.html

4 Codes d'exploitation via une page Web et détection réseau

Il existe de nombreuses vulnérabilités liées à des codes dynamiques (ActiveX, JavaScript, Flash) ou des vulnérabilités intrinsèques au navigateur (interprétation des URIs, gestion des balises, redirection par des *iframes* frauduleuses, etc.).

Certaines mesures de surveillance consistent alors à mettre un équipement réseau, par exemple une sonde de détection d'intrusion, afin de surveiller et d'alerter l'administrateur à la vue d'une tentative d'exploitation.

Il apparaît que plusieurs de ces équipements s'appuient :

- sur les communications impliquant un port bien particulier (port 80/TCP principalement) ;
- sur les échanges HTTP présentant des caractéristiques particulières (réponse code 200 précédent un échange) ;
- etc.

Que se passe-t-il pour les pages HTML servies en FTP ?

Dans une négociation normale, l'échange sera de la forme (C représente le poste utilisé pour naviguer, et S le serveur hébergeant le site Web) :

```
(C)  FTP: Request: USER anonymous  -->            (S)

(C)  <-- FTP: Response:220 xxxxxx Server          (S)

(C)  <-- FTP:  Response:331 Anonymous login ok    (S)

(C) FTP: Request: PASS xxx@yyyyyy                 (S)

(C) <-- FTP: Response:230 Anonymous access granted (S)

(C) FTP: Request: SYST -->                        (S)

(C) <-- FTP:Response:215 UNIX Type:L8             (S)

(C) FTP: Request: PWD -->                         (S)
```

```
(C) <-- FTP:Response:257 "/" is current directory  (S)

(C) FTP:Request: TYPE I  -->                      (S)

(C) <-- FTP:Response:200 Type set to I            (S)

(C) FTP:Request: CWD xxxxxxx -->                  (S)

(C) <-- FTP:Response:250 CWD command successful   (S)

(C) FTP:Request: PASV -->                         (S)

(C) <-- FTP:Response: 227 Entering Passive Mode   (S)

(C) FTP:Request: SIZE MaPage.html -->             (S)

(C) <-- FTP:Response:213 xxxx                     (S)

(C) FTP:Request: RETR xxxxxxxxx/MaPage.html -->   (S)

(C) <-- FTP:Response:150 Opening BINARY mode data  (S)

(C) <-- FTP DATA: xxx byte                        (S)
(...)
(C) <-- FTP DATA: xxx byte                        (S)

(C) <-- FTP:Response:226 Transfer complete        (S)
```

Dans la situation ci-dessus, en mode FTP passif, il est difficile de connaître les ports d'échange de données *a priori*. Le client utilise pour le transfert de données un port non privilégié. Le serveur fait de même en indiquant dans sa réponse (227) son nouveau port en écoute pour le transfert de données.

Les mesures de détection précédemment citées s'avèrent inutiles, à moins d'inspecter l'ensemble des trames en transit ou de surveiller les échanges FTP.

En revanche, le navigateur ne fera pas la distinction sur le protocole qui a été utilisé, HTTP ou FTP. Il interprétera dans les deux cas le code source de la page récupérée. L'exploitation de la vulnérabilité peut réussir sans que le système de détection n'émette la moindre alerte. La problématique est identique avec l'ouverture locale du fichier HTML malveillant ou via des protocoles moins courants comme Gopher[1], etc.

Tous les équipements de sécurité n'ont évidemment pas cette caractéristique, mais cela permet de rappeler quelques points particuliers :

- la présence d'outils de surveillance réseau ne doit en aucun cas faire oublier l'impérative nécessité de mettre à jour ses applications et ses systèmes d'exploitation. Le principe de défense en profondeur implique, *a priori*, d'appliquer toutes les mesures de défense les plus élémentaires ;
- tout équipement de sécurité doit être maîtrisé. Il n'y a aucune magie dans leur fonctionnement, qu'il faut connaître afin de déterminer les limites du service rendu.

5 IPv6 et configuration

La plupart des systèmes d'exploitation propriétaires ou libres récents mettent en œuvre une pile IPv6. Le CERTA a déjà détaillé dans la note d'information CERTA-2006-INF-004 les risques et principaux enjeux de sécurité ayant trait à ce protocole. Récemment, le CERTA a recontré un problème sur un serveur de messagerie qui « s'obstinait » à ne pas vouloir relayer des messages provenant de son domaine légitime ou de lui-même alors que la configuration, vérifiée par l'administrateur puis par le CERTA, semblait correcte. S'il est besoin de rappeler l'utilité des journaux d'événements, c'est dans ceux du serveur que l'on pouvait trouver un début d'explication. On pouvait lire dans les lignes de rejet la chaîne suivante :

```
NOQUEUE: reject: RCPT from ::1
```

[1] Il faut cependant noter que Gopher n'est plus supporté par défaut par tous les navigateurs, en particulier par Internet Explorer.

Dans le cas présent, cette seule information pouvait être suffisante pour expliquer le problème. En effet, cet extrait indique que le serveur voulait envoyer un message en présentant son adresse IPv6 de bouclage. Or le relais de messagerie était configuré pour relayer exclusivement des messages provenant de réseaux en IPv4 bien que supportant l'IPv6. Recevant des messages depuis une adresse en IPv6, le serveur n'acceptait pas de les prendre en charge car aucune adresse IPv6 n'était précisée dans les réseaux autorisés à utiliser le serveur. Il a suffi alors de spécifier dans la configuration du serveur de ne pas mettre en œuvre dans son traitement les adresses de type IPv6 et de ne s'attacher qu'aux adresses IPv4 pour corriger le problème.

Recommandations :

L'IPv6 bien que mis en oeuvre au niveau du système d'exploitation est parfois mal pris en charge par les applications ou les services réseaux en particulier dans leur configuration par défaut. Lors de l'installation et la configuration d'une machine, il faudra toujours s'attacher à bien configurer la partie IPv6 d'un service. Si ce protocole n'est pas utilisé, il conviendra de bien positionnner la directive désactivant son support dans la configuration de l'application afin d'éviter une configuration trop laxiste ou des effets secondaires indésirables.

6 Lecture des journaux Web, la requête HEAD

Cette semaine, le CERTA a reçu eu plusieurs questions sur la signification des requêtes `HEAD` dans les journaux de serveurs Web. Voyons dans cet article de quoi il s'agit.

Les requêtes `HEAD` se trouvent dans les journaux des serveurs Web noyées au milieu de celles plus connues telles que `POST` et `GET`. Une requête `HEAD` permet d'obtenir d'un serveur les mêmes méta-données qu'il aurait servi, avec le contenu, en réponse à une requête `GET`. Elle peut être utilisée, entre autres, pour tester l'existence d'une page (code retour 200) ou vérifier l'obsolescence d'un contenu afin de le mettre à jour, par exemple, au niveau d'un serveur mandataire (champs *last-modified*, *content-length* et *Age*). Les méta-données retournées contiennent aussi des informations permettant d'en apprendre plus sur le serveur (*fingerprinting*). Son intérêt par rapport à une requête `GET` classique est qu'elle génère beaucoup moins de volume de trafic et permet donc de tester rapidement la configuration d'un serveur ou l'existence de nombreuses pages, à des fins légitimes, ou pas. La présence de telles traces dans les journaux peut donc avoir plusieurs explications, que seule une étude au cas par cas permet de définir.

6.1 Documentation

– RFC 2616 Section 9 «Method Definitions»
http://www.w3.org/Protocols/rfc2616/rfc2616-sec9.html

7 Ports observés

Le tableau 3 et la figure 1 montrent les rejets pour les ports sous surveillance que nous avons constatés sur des dispositifs de filtrage, entre le 05 et le 12 février 2009.

8 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/

9 Rappel des avis émis

Dans la période du 06 au 13 février 2009, le CERTA a émis les avis suivants :

- CERTA-2009-AVI-051 : Multiples vulnérabilités dans les Cisco Wireless LAN Controllers
- CERTA-2009-AVI-052 : Multiples vulnérabilités du système SCADA e-terrahabitat d'AREVA
- CERTA-2009-AVI-053 : Vulnérabilité dans HP OpenView Network Node Manager
- CERTA-2009-AVI-054 : Vulnérabilités de Trend Micro Interscan Web Security Suite
- CERTA-2009-AVI-055 : Vulnérabilités dans Wireshark
- CERTA-2009-AVI-056 : Vulnérabilité de la pile IPv6 dans Sun Solaris
- CERTA-2009-AVI-057 : Vulnérabilité dans Sun Solaris RPC
- CERTA-2009-AVI-058 : Vulnérabilité dans HP LaserJet et HP Digital Sender
- CERTA-2009-AVI-059 : Vulnérabilités dans Microsoft Internet Explorer
- CERTA-2009-AVI-060 : Multiples vulnérabilités dans Microsoft Exchange
- CERTA-2009-AVI-061 : Vulnérabilité dans Microsoft SQL Server
- CERTA-2009-AVI-062 : Multiples vulnérabilités dans Microsoft Visio
- CERTA-2009-AVI-063 : Vulnérabilités de TYPO3
- CERTA-2009-AVI-064 : Vulnérabilité dans l'Autorun sur Windows
- CERTA-2009-AVI-065 : Vulnérabilité de la commande sudo

10 Actions suggérées

10.1 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.

10.2 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.

10.3 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.

10.4 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.

10.5 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.

10.6 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.

10.7 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.ssi.gouv.fr/fr/formation/

11 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.

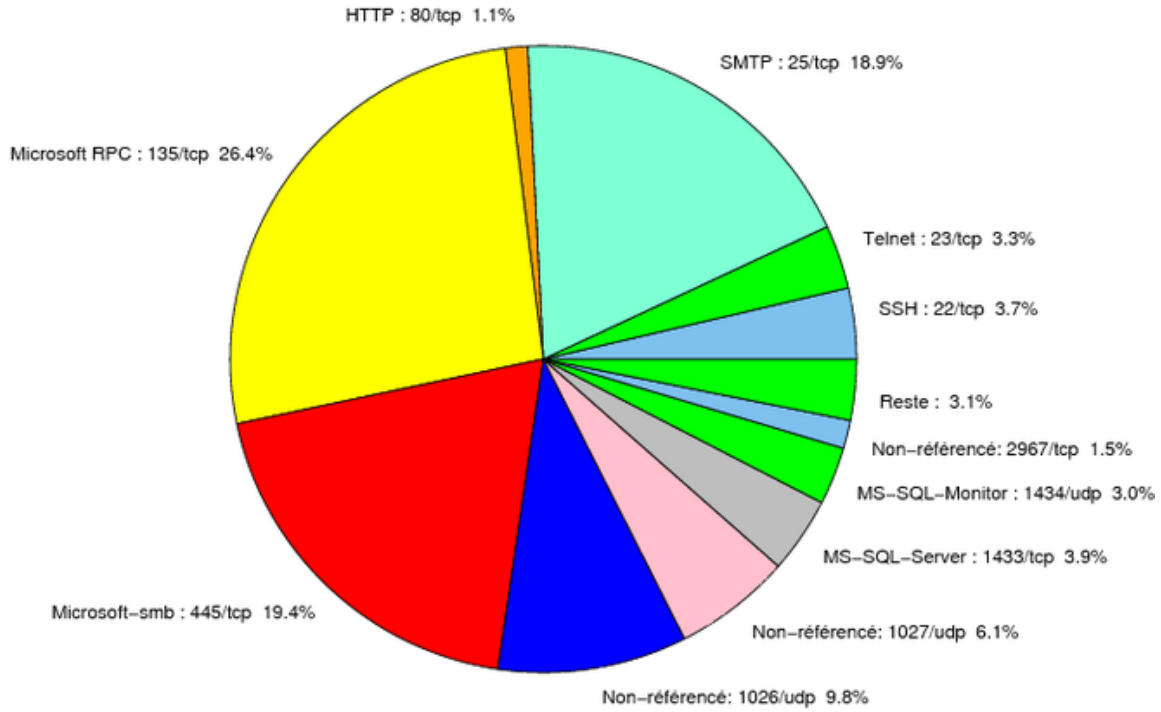

FIG. 1: Répartition relative des ports pour la semaine du 05.02.2009 au 12.02.2009

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	26.37
445/tcp	19.37
25/tcp	18.85
1026/udp	9.76
1027/udp	6.05
1433/tcp	3.91
22/tcp	3.65
23/tcp	3.28
1434/udp	2.97
2967/tcp	1.46
80/tcp	1.14
139/tcp	0.93
4899/tcp	0.88
21/tcp	0.83
137/udp	0.2
3389/tcp	0.15
2100/tcp	0.1

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

13 février 2009 version initiale.