

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2008-28

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-2008-ACT-028>

Gestion du document

Référence	CERTA-2008-ACT-028
Titre	Bulletin d'actualité 2008-28
Date de la première version	11 juillet 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-028.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-028/>

1 Retours sur les événements associés au DNS

1.1 Introduction

La presse a très largement relayé cette semaine une vulnérabilité importante concernant DNS. Le *Domain Name System* est un élément important de l'architecture Internet puisqu'il assure la transposition des noms de machine en adresse IP, sur lesquelles s'effectue le routage. Le CERTA revient sur cet événement et les faits associés.

Un chercheur a annoncé une vulnérabilité protocolaire du DNS pouvant conduire à une corruption du cache. Il ne fournira cependant les détails techniques de celle-ci qu'au début du mois d'août à l'occasion d'une conférence. Cette annonce avait fait depuis quelques jours l'objet de rumeurs.

Mardi 08 juillet au soir, plusieurs éditeurs ont publié simultanément des correctifs de leur mise en œuvre du DNS. On peut citer à valeur d'exemple :

- ISC Bind (CERTA-2008-AVI-359)
- Cisco (CERTA-2008-AVI-358)
- Microsoft (CERTA-2008-AVI-353)
- Juniper (CERTA-2008-AVI-360)

D'autres mises à jour devraient progressivement apparaître dans les prochains jours.

1.2 Que font ces mises à jour ?

Il est bien important de comprendre ici qu'elles ne corrigent pas la vulnérabilité protocolaire annoncée mais restreignent les possibilités de réussir son exploitation. Il s'agit pour cela d'empêcher à une personne malveillante de pouvoir construire de fausses réponses spécifiques réalistes. Or les réponses DNS fonctionnent généralement sur la couche de transport UDP, protocole sans état. Les seules méthodes possibles pour complexifier la construction de trames malveillantes consistent ainsi à rendre certains champs de celle-ci difficilement prédictibles en augmentant leur entropie.

Les premiers standards mentionnant le DNS datent du début des années 1980 (1982) :

<http://www.dns.net/dnsrd/rfc/>

Ceux qui servent de référence sont les RFC 1034 et 1035 rédigés par P. Mockapetris en 1987. En 1995, P. Vixie publiait dans une conférence un article intitulé « DNS and BIND Security Issues » le commentaire suivant :

6. What We Cannot Fix

(...)

With only 16 bits worth of query ID and 16 bits worth of UDP port number, it's hard not to be predictable. A determined attacker can try all the numbers in a very short time and can use patterns derived from examination of the freely available BIND source code. Even if we had a white noise generator to help randomize our numbers, it's just too easy to try them all.

http://www.usenix.org/publications/library/proceedings/security95/full_papers/vixie.txt

En d'autres termes, l'auteur de cet article précise que les champs qui peuvent être utilisés sont l'identifiant de transaction et le port source de la requête. Ceux-ci ne seront par ailleurs jamais à eux-seuls suffisants pour rendre la réponse impossible à prédire.

Des mises en œuvre DNS ont appliqué ces mesures. D'autres les ont appliquées partiellement en se limitant à rendre aléatoire les identifiants de transaction ; les ports source sont quasi-invariants et prédictibles. C'est le cas de BIND qui choisit un port source aléatoire mais le conserve ensuite jusqu'au prochain redémarrage du service.

Sans mentionner ici les problèmes liés à la propre génération de valeurs aléatoires des identifiants qui a fait l'objet de plusieurs correctifs en 2007, il faut rappeler ici quelques résultats de probabilités publiés en 2001 par l'auteur de *djbdns* (serveur DNS), D.J. Bernstein, défendant alors l'intérêt d'utiliser des ports source aléatoires. Les chiffres représentés sont le nombre de paquets maximaux nécessaires en fonction des aléas utilisés:

	Attaque aveugle brute -----	Attaque aveugle Collision -----	Attaque par capture de trames (sniff) -----
Aucun	1	1	1
ID (BIND)	65536	256	1
ID+port (djbdns)	4227727360	65020	1

D'autres chiffres peuvent être fournis en appliquant de manière brute des formules du paradoxe des anniversaires. Les ordres de grandeur restent néanmoins similaires.

Les correctifs publiés appliquent un ensemble de bonnes pratiques préconisées depuis quelques années. Le fait d'introduire de l'aléa pour les ports source n'est pas sans poser un certain nombre de problèmes relatifs aux pare-feux. Certains pare-feux personnels ne prennent pas en compte cette modification de comportement et bloquent les réponses pourtant légitimes.

1.3 Foire aux questions

Question n°1 : Quelle est la nature du problème DNS qui a été largement médiatisé cette semaine ?

Lorsqu'un serveur DNS envoie une requête à un autre serveur, il attend une réponse qui contiendra des informations correspondants à sa demande et en particulier :

- le port destinataire de la réponse doit correspondre au port source de la requête ;

- l'identifiant de transaction dans la réponse doit être le même que celui de la requête.

Comme le choix de ces deux facteurs était relativement facilement prédictible, il devenait possible de créer une fausse réponse correspondant à une vraie requête et donc de corrompre le cache du DNS. Les correctifs de sécurité diffusés cette semaine améliorent la génération pseudo aléatoire de ces facteurs.

Question n°2 : La vulnérabilité DNS est-elle grave ?

Les vulnérabilités touchant le DNS sont de fait graves car elles peuvent provoquer d'importants dysfonctionnements de l'Internet. En l'occurrence, dans cette affaire le risque est de tromper l'utilisateur en l'envoyant de façon silencieuse vers un faux site.

Question n°3 : Que faut-il faire pour limiter les risques ?

Il convient d'appliquer sans délais les correctifs de sécurité et de vérifier la bonne configuration des serveurs DNS. A ce propos, un serveur DNS ne doit être récursif que pour le domaine dont il a la responsabilité. Un DNS ne doit répondre à l'Internet que pour les zones sur lesquelles il a autorité.

Question n°4 : Il a été dit que la vulnérabilité était protocolaire : cela signifie quoi ?

Cela signifie que cette vulnérabilité n'est pas liée à une mise en œuvre particulière dans un logiciel donné. Simplement, les logiciels peuvent en atténuer les risques par des mesures appropriées comme un choix plus aléatoire des ports sources. L'attaque est donc probabiliste. Les spécifications du protocole DNS n'ont pas prévu la situation mise en évidence par la vulnérabilité.

Question n°5 : Les serveurs d'autorité de la zone « .fr » sont-ils concernés ?

Non. Ces serveurs ne sont pas concernés car ils ne sont pas récursifs.

1.4 Conclusion

Il faut bien comprendre que la corruption de cache DNS est difficilement visible par l'utilisateur. S'il détecte un comportement anormal, il ne sera pas en mesure d'identifier simplement si le problème vient du DNS ou du site qu'il visite, par exemple.

Il appartient aux administrateurs des serveurs de prendre des mesures. Un ensemble de bonnes pratiques doit être impérativement appliqué :

- mettre à jour les serveurs DNS ;
- vérifier la configuration de ces derniers pour cloisonner les fonctions (modes itératifs ou récursifs, mises en cache, etc.) et limiter en particulier le mode « récursif » aux plages d'adresses IP légitimes, voir à ce sujet le bulletin d'actualité du CERTA CERTA-2008-ACT-008 du 22 février 2008 ;
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-008>
- appliquer des politiques de filtrage réseau rigoureuses pour le trafic DNS ;
- journaliser et regarder régulièrement les journaux ;
- surveiller le trafic réseau afin de détecter toute activité anormale, en particulier :
 - des pics de trafic non justifiés ;
 - des réponses DNS possédant les mêmes caractéristiques (identifiant de transaction, IP/port source) mais des enregistrements distincts.

Le CERTA tiendra publiera dans les prochains jours une note d'information rappelant un ensemble de risques et de bonnes pratiques liées au DNS.

2 Incident de la semaine

2.1 Campagne d'ingénierie sociale

Cette semaine, le CERTA a été informé d'une campagne d'ingénierie sociale visant plusieurs administrations. Cette campagne tente, par l'envoi de courriels, de récupérer les identifiants et mots de passe d'utilisateurs.

Toutes les administrations visées ont pour point commun l'utilisation d'une application de gestion de contenu intégrant un *webmail*, *Horde*. Une fois les données d'un compte utilisateur récupérées, ce compte est utilisé à d'autres fins malveillantes :

- soit pour effectuer une autre campagne d'ingénierie sociale vers d'autres organismes ;
- soit pour l'envoi de courriels indésirables.

Le CERTA tient donc à attirer l'attention de ses lecteurs sur la nécessité de sensibiliser les utilisateurs du système d'information des risques associés à l'ingénierie sociale. En effet, il ne faut jamais fournir ces identifiants et mots de passe.

De plus, il est fortement conseillé d'analyser de manière régulière les journaux de connexions des applications de ce type et de prêter une attention toute particulière aux connexions suspectes, comme celles provenant par exemple de l'étranger ou faites à des heures non conventionnelles.

2.2 Les applications client-serveur

Cette semaine, le CERTA a été contacté concernant un problème de sécurité potentiel sur une application client-serveur. Cette application, développée spécifiquement pour une administration, permet d'accéder à certaines informations présentes dans une base de données. Le compte permettant l'accès à la base de données a été défini directement dans le binaire de la partie cliente de l'application. Ce compte ne dispose pas de droit limité sur les données, l'application étant censée restreindre les accès. De plus, le protocole utilisé pour la communication entre le client et le serveur n'est pas chiffré.

Il devient donc possible à une personne malintentionnée de réaliser une analyse inverse du code de l'application cliente pour retrouver les identifiants de connexion à la base de données, contournant ainsi la « mesure » de protection mise en oeuvre. L'utilisation d'un protocole non-chiffré peut également permettre, en écoutant le réseau (en utilisant un *sniffeur*), de retrouver le compte utilisé ou d'intercepter les données échangées.

Une personne malveillante disposant du compte utilisé par l'application pourrait interroger directement le serveur de base de données et ainsi accéder à des informations non-autorisées.

Le CERTA recommande de ne pas utiliser de comptes générique car cette pratique rend difficile l'identification *a posteriori*. Les comptes utilisés doivent être restreints, ne permettant pas de modifier, supprimer ou accéder à des données non-autorisées. Le fait de figer dans une application un mot de passe ne permet pas de le mettre à jour facilement et régulièrement. Cette pratique peut être contraire à la politique de gestion des mots de passe mise en oeuvre au sein du système d'information.

Documentation

- Note d'information du CERTA sur les bons réflexes en cas d'intrusion sur un système d'information : <http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-002/>
- Note d'information du CERTA sur les mots de passe : <http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/>

3 Vulnérabilités dans des produits Microsoft

Le CERTA a publié cette semaine deux alertes sur des produits Microsoft. Celles-ci concernent des failles non corrigées et actuellement exploitées de Microsoft Office Word et Microsoft Office Access.

3.1 Vulnérabilité dans Microsoft Office Access

La première vulnérabilité a fait l'objet de l'alerte CERTA-2008-ALE-009 et concerne le contrôle ActiveX du Snapshot Viewer for Microsoft Access. La faille permet à une personne malintentionnée de forcer le téléchargement d'un fichier vers un répertoire arbitraire du poste de l'utilisateur, selon ses droits.

Le contrôle vulnérable est installé par défaut avec les versions 2000, XP et 2003 de Microsoft Access. Il est également signé par Microsoft, ce qui signifie qu'il peut être téléchargé automatiquement dans certaines configurations (« Télécharger les contrôles ActiveX signés ») et/ou exécuté automatiquement (« Exécuter les contrôles ActiveX et les plug-ins »).

L'un des contournements de la vulnérabilité est justement de migrer si nécessaire vers Internet Explorer 7 et de mettre ces options à « Demander ».

Il est également possible et fortement recommandé de désactiver le contrôle ActiveX vulnérable (cf. CERTA-2008-ALE-009) ou d'utiliser un navigateur alternatif. La navigation avec un compte aux droits restreints et limités à des sites uniquement de confiance est également une bonne pratique.

Pour les administrateurs, il est possible de filtrer avec un serveur mandataire inverse les chaînes suivantes :

```
F0E42D50-368C-11D0-AD81-00A0C90DC8D9  
F0E42D60-368C-11D0-AD81-00A0C90DC8D9  
F2175210-368C-11D0-AD81-00A0C90DC8D9
```

3.2 Vulnérabilité dans Microsoft Office Word

La vulnérabilité dans Microsoft Office Word a fait l'objet de l'alerte CERTA-2008-ALE-010. La faille permet à une personne d'exécuter du code arbitraire sur le poste d'une victime après ouverture d'un fichier spécialement conçu.

Seul Microsoft Office Word 2002 est concerné.

Les contournements sont l'utilisation d'autres logiciels, tels que :

- Microsoft Office Word 2003 ou 2007 ;
- Openoffice.org ;
- Word Viewer 2003 SP3.

3.3 Documentation

- Alerte CERTA-2008-ALE-009 du 08 juillet 2008
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-ALE-009/index.html>
- Alerte CERTA-2008-ALE-010 du 09 juillet 2008
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-ALE-010/index.html>

4 Problème avec certains produits Sophos

Une mise à jour de juillet de la base des signatures de virus (4.31) et du moteur (2.75) pour certains produits *Sophos* provoque des arrêts inopinés lors du traitement de certains éléments MIME ayant une longueur nulle.

Les produits affectés sont :

- *Sophos Email Appliance* ;
- *Pure Message for Unix* ;
- *Sophos Anti-Virus Interface (SAVI)*.

Apparemment, seules les versions pour Linux/Unix sont concernées.

Une mise à jour automatique pour *Sophos Email Appliance* et *Pure Message for Unix* a ramené la base de signatures en version 4.30 et le moteur en version 2.74. Concernant *SAVI*, un correctif a été appliqué automatiquement lors d'une mise à jour.

Documentation :

- Bulletin de sécurité Sophos du 09 juillet 2008 :
<http://www.sophos.com/support/knowledgebase/article/42245.html>

5 Le projet Weave

La fondation *Mozilla* a sorti, à la fin de l'année 2007, un nouveau module additionnel pour son navigateur, *Weave*.

Cette extension a pour but d'exporter vers l'Internet l'ensemble des données relatives à la navigation d'un utilisateur :

- marque-pages ;
- historique de navigation ;
- mots de passe ;
- éléments de personnalisation ;
- etc.

Ainsi un utilisateur pourra retrouver toutes les informations dont il a l'habitude, sur n'importe quelle machine, du moment qu'elle est pourvue du navigateur et de l'extension de la fondation *Mozilla*. Ces informations sont accessibles après une authentification et les données sont chiffrées sur le poste client afin de limiter les possibilités

de récupération par un autre utilisateur. En plus de centraliser l'ensemble de ces éléments, il existe la possibilité de partager et de déléguer la gestion de tout ou partie de ces informations à des tiers.

Malgré l'aspect pratique de ce type d'application, le CERTA tient à rappeler que les données personnelles de l'utilisateur sont stockés sur des serveurs dont il n'a pas le contrôle. Il est donc possible que des données soient récupérées par des personnes et/ou organismes auxquels il ne voulait pas les communiquer. Le CERTA ne recommande pas d'utiliser ce type de module pour les raisons suivantes :

- l'ajout d'extension à une application augmente le risque de vulnérabilité. Si le module est vulnérable, il devient alors une porte d'entrée intéressante pour des personnes malveillantes vu les données manipulées par ce dernier ;
- le fait de mettre toutes les données personnelles sous le protection d'un compte unique affaiblit de manière générale le niveau de sécurité et peut faciliter le vol de données si le compte est compromis.

6 Les protections de *Firefox 3*

Les fonctionnalités de protection sont le résultat de l'intégration de l'extension *Safe Browsing* développée par *Google* dans *Firefox 2*. Elles se sont enrichies avec la version 3 du navigateur en apportant en plus d'une protection contre les sites contrefaits (filoutage), une protection contre les sites malveillants. Elles fonctionnent sur un principe de *listes (noires ou blanches)* enregistrées localement et régulièrement mises à jour. Ces listes contiennent les *hash* partiels des URL suspects.

6.1 Les mises à jour des listes

Cette nouvelle version apporte une modification de la gestion des mises à jour. Il ne s'agit plus de maintenir des listes dans leur totalité mais de maintenir des bouts de liste, les *chunks*. Ils possèdent un identifiant unique et décrivent les informations à rajouter ou à retirer des listes. Pour effectuer une mise à jour, le navigateur annonce la liste qu'il veut mettre à jour et les *chunks* associés qu'il possède. Le serveur lui répond les *chunks* obsolètes pour chaque liste et les URL où il pourra télécharger les nouveaux *chunks*.

Par exemple, le navigateur annonce qu'il a déjà les *chunks add 1-3,5,8* et les *chunks sub 4-5*, pour la liste *goog-phish-shavar* soit:

```
goog-phish-shavar;a:1-3,5,8;s:4-5
```

Le serveur répond que les *chunks sub 1* et *2* sont obsolètes et l'adresse où télécharger les nouveaux disponibles :

```
n:1200
```

```
i:goog-phish-shavar
```

```
u: cache.google.com/first
```

```
sd:1,2
```

La connexion à *cache.google.com/first* retourne une liste de *chunks* et les données associées:

```
a:4:48:1200
```

```
[encoded data]
```

```
s:3:96:100
```

```
[encoded data]
```

```
a:6:32:800
```

```
[encoded data]
```

```
a:7:48:1200
```

```
[encoded data]
```

Toutes ces informations sont enregistrées dans le fichier de base de données *urlclassifier3.sqlite*

6.2 La base *urlclassifier3.sqlite*

Elle contient trois tables. Les deux premières *moz_classifier* et *moz_subs* contiennent des hash partiels d'URL et les *chunks* de provenance. Dans la table *moz_tables* on trouve les colonnes *id*, *name*, *add_chunks* et *sub_chunks*, qui correspondent aux listes et leurs formats, ainsi que la liste des *chunks* de type *add* ou *sub*. Le détail du format des données enregistrées semble encore très confidentiel et très peu d'informations sont disponibles, contrairement à la version précédente où les URL étaient chiffrées en ROT13. Il est

possible de lire ces fichiers avec des outils tels que *SQLite Database Browser* ou en ligne avec une commande ressemblant à :

```
echo "SELECT * FROM goog-phish-shavar LIMIT 10;" | sqlite3
urlclassifier3.sqlite
```

Les URL contenues dans la version précédente, `urlclassifier2.sqlite` étaient chiffrées en ROT13 et étaient lisibles avec la commande :

```
echo "SELECT key FROM goog_black_url LIMIT 10;" | sqlite3
urlclassifier2.sqlite | tr N-ZA-Mn-za-m A-Za-z
```

6.3 Documentation

- *Phishing Protections: Server Spec*
<http://code.google.com/p/google-safe-browsing/wiki/Protocolv2Spec>
- *Google Safe Browsing - spec v2*
http://wiki.mozilla.org/Phishing_Protection:_Design_Documentation

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 03 et le 10 juillet 2008.

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 04 au 10 juillet 2008, le CERTA a émis les avis suivants :

- CERTA-2008-AVI-347 : Vulnérabilité de Sun Java System Access Manager

- CERTA-2008-AVI-348 : Vulnérabilité dans VLC Media Player
- CERTA-2008-AVI-349 : Multiples vulnérabilités dans Sun Solaris
- CERTA-2008-AVI-350 : Multiples vulnérabilités dans Firefox 2
- CERTA-2008-AVI-351 : Vulnérabilité de Sun Solaris
- CERTA-2008-AVI-352 : Vulnérabilités dans Avaya Call Management System
- CERTA-2008-AVI-353 : Vulnérabilité DNS dans Microsoft Windows
- CERTA-2008-AVI-354 : Vulnérabilité de l'explorateur de fichiers Windows
- CERTA-2008-AVI-355 : Vulnérabilités dans Open Web Access
- CERTA-2008-AVI-356 : Multiples vulnérabilités dans Microsoft SQL Server
- CERTA-2008-AVI-357 : Vulnérabilités dans Joomla!
- CERTA-2008-AVI-358 : Vulnérabilité dans les produits Cisco
- CERTA-2008-AVI-360 : Vulnérabilité dans l'implémentation du protocole DNS par Juniper
- CERTA-2008-AVI-361 : Vulnérabilité dans PCRE
- CERTA-2008-AVI-362 : Vulnérabilités dans Opera
- CERTA-2008-AVI-363 : Vulnérabilité dans Novell eDirectory

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

- CERTA-2008-AVI-331-001 : Vulnérabilité du navigateur Safari
(ajout d'une référence au bulletin d'Apple sur MacOS et mise à jour de la description)
- CERTA-2008-AVI-359-001 : Vulnérabilités dans ISC BIND
(ajout des références au CVE et aux bulletins de sécurité Debian, Red Hat et Sun)

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 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.

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 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.

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.formation.ssi.gouv.fr>

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.

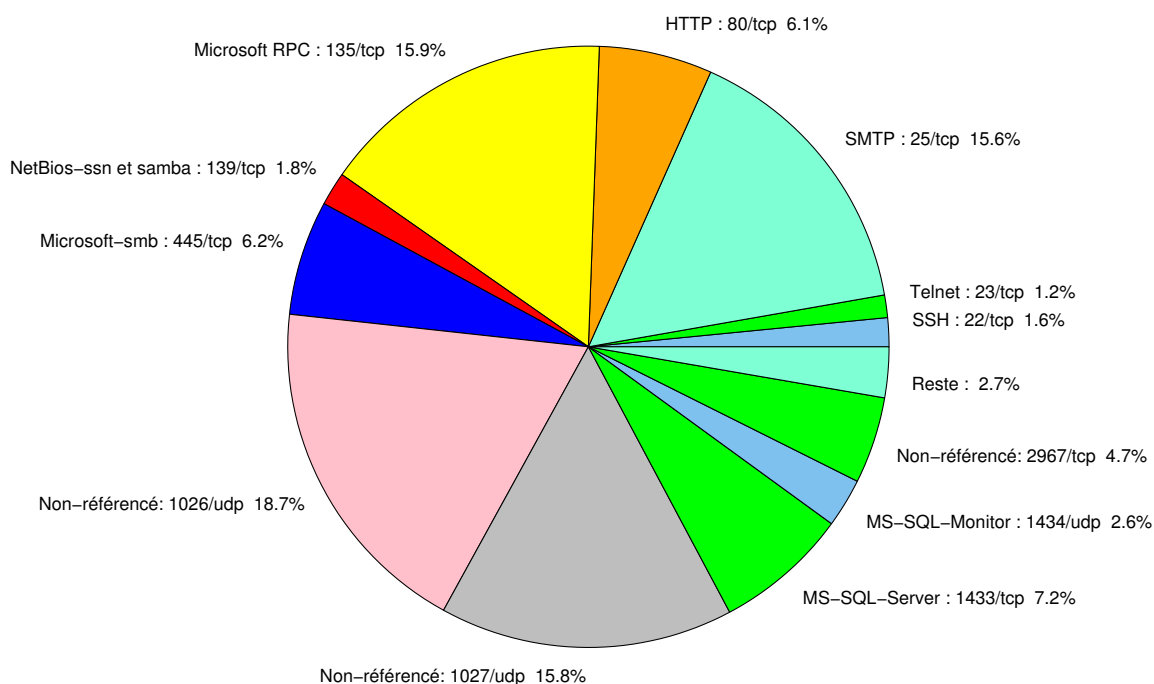


FIG. 1: Répartition relative des ports pour la semaine du 03.07.2008 au 10.07.2008

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	-	CERTA-2003-AVI-132 CERTA-2004-AVI-064 CERTA-2004-AVI-066 CERTA-2006-AVI-040
22	TCP	SSH	-	CERTA-2003-AVI-152 CERTA-2006-AVI-100
23	TCP	Telnet	-	CERTA-2003-AVI-209 CERTA-2003-AVI-131 CERTA-2007-ALE-005-001
25	TCP	SMTP	-	CERTA-2006-AVI-124 CERTA-2006-AVI-135
42	TCP	WINS	-	CERTA-2004-AVI-384
69	UDP	IBM Tivoli Provisioning Manager	-	CERTA-2007-AVI-320
80	TCP	HTTP	-	CERTA-2004-AVI-195 CERTA-2004-AVI-239 CERTA-2006-AVI-055 CERTA-2006-AVI-069 CERTA-2006-AVI-156 CERTA-2006-AVI-315
106	TCP	MailSite Email Server	-	- CERTA-2007-AVI-008
111	TCP	Sunrpc-portmapper	-	CERTA-2003-AVI-052
119	TCP	NNTP	-	CERTA-2004-AVI-340
135	TCP	Microsoft RPC	-	CERTA-2003-ALE-002 CERTA-2003-AVI-111 CERTA-2004-AVI-127
137	UDP	NetBios-ns	-	CERTA-2004-AVI-031
139	TCP	NetBios-ssn et samba	-	CERTA-2004-AVI-368 CERTA-2003-AVI-168 CERTA-2004-AVI-126 CERTA-2005-AVI-051

				CERTA-2005-AVI-213 CERTA-2005-AVI-302 CERTA-2005-AVI-398 CERTA-2006-AVI-283 CERTA-2006-AVI-338 CERTA-2007-AVI-321
143	TCP	IMAP	–	CERTA-2005-AVI-185
389	TCP	LDAP	–	CERTA-2003-AVI-102 CERTA-2003-AVI-068 CERTA-2003-AVI-041 CERTA-2003-AVI-004 CERTA-2004-AVI-126 CERTA-2007-AVI-294
427	TCP	Novell Client	–	CERTA-2006-AVI-538
443	TCP	HTTPS	–	CERTA-2003-AVI-156 CERTA-2004-AVI-126 CERTA-2004-AVI-247 CERTA-2004-AVI-343 CERTA-2007-AVI-153
445	TCP	Microsoft-smb	–	CERTA-2004-AVI-053 CERTA-2003-AVI-105 CERTA-2004-AVI-126 CERTA-2005-AVI-051 CERTA-2005-AVI-302 CERTA-2006-AVI-283 CERTA-2006-AVI-338 CERTA-2007-AVI-321 CERTA-2007-ALE-010
445	UDP	Microsoft-smb	–	CERTA-2007-ALE-010
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	CERTA-2006-AVI-232
1433	TCP	MS-SQL-Server	–	CERTA-2002-ALE-006
1434	UDP	MS-SQL-Monitor	–	CERTA-2002-AVI-157
2100	TCP	Oracle XDB FTP	–	CERTA-2005-ALE-002
2381	TCP	HP System Management	–	CERTA-2006-AVI-248
2512	TCP	Citrix MetaFrame	–	CERTA-2006-AVI-491
2513	TCP	Citrix MetaFrame	–	CERTA-2006-AVI-491
2745	TCP	–	Bagle	–
2967	TCP	Symantec Antivirus	Yellow Worm	CERTA-2006-AVI-221
3104	TCP	CA Message Queuing	–	CERTA-2007-AVI-331
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	CERTA-2004-AVI-062 CERTA-2004-AVI-186 CERTA-2004-AVI-316 CERTA-2004-AVI-348
3268	TCP	Microsoft Active Directory	–	CERTA-2007-AVI-294
3306	TCP	MySQL	–	–
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	CERTA-2001-AVI-165 CERTA-2006-AVI-212 CERTA-2006-AVI-297
5151	UDP	IPSwitch WS_TP	–	CERTA-2007-AVI-312
5151	TCP	ESRI ArcSDE	–	CERTA-2007-AVI-367
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	CERTA-2006-AVI-198 CERTA-2006-AVI-299
6014	TCP	IBM Tivoli Monitoring	–	CERTA-2007-AVI-183

6070	TCP	BrightStor ARCserve/Enterprise Backup	–	CERTA-2005-AVI-293
6101	TCP	Veritas Backup Exec	–	CERTA-2005-AVI-024
6106	TCP	Symantec Backup Exec	–	CERTA-2007-AVI-303
6129	TCP	Dameware Miniremote	–	CERTA-2003-AVI-214 CERTA-2005-AVI-326
6502	TCP	CA BrightStor ARCserve Backup	–	CERTA-2007-AVI-029
6503	TCP	CA BrightStor ARCserve Backup	–	CERTA-2007-AVI-029
6504	TCP	CA BrightStor ARCserve Backup	–	CERTA-2007-AVI-029
8080	TCP	IBM Tivoli Provisioning Manager	–	CERTA-2007-AVI-153
8866	TCP	–	Porte dérobée Bagle.B	–
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	CERTA-2005-AVI-229 CERTA-2005-AVI-313
10080	TCP	Amanda	MyDoom	–
10110	TCP	IBM Tivoli Monitoring	–	CERTA-2007-AVI-183
10916	TCP	Ingres	–	CERTA-2007-AVI-275-001
10925	TCP	Ingres	–	CERTA-2007-AVI-275-001
12168	TCP	CA eTrust antivirus	–	CERTA-2007-AVI-217
13701	TCP	Veritas NetBackup	–	CERTA-2005-AVI-447
18264	TCP	CheckPoint interface	–	CERTA-2005-AVI-310
54345	TCP	HP Mercury	–	CERTA-2007-AVI-075
65535	UDP	LANDesk Management Suite	–	CERTA-2007-AVI-176

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

port	pourcentage
1026/udp	18.72
135/tcp	16
1027/udp	15.78
25/tcp	15.57
1433/tcp	7.2
445/tcp	6.16
80/tcp	6.12
2967/tcp	4.65
1434/udp	2.63
139/tcp	1.81
22/tcp	1.55
23/tcp	1.38
4899/tcp	0.77
137/udp	0.6
1080/tcp	0.51
3128/tcp	0.38
21/tcp	0.17
3389/tcp	0.12
2100/tcp	0.08
3306/tcp	0.04

TAB. 3: Paquets rejetés

Liste des tableaux

1	Gestion du document	1
2	Correctifs correspondant aux ports destination des paquets rejetés	12
3	Paquets rejetés	13

Gestion détaillée du document

11 juillet 2008 version initiale.