Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 04 mars 2011
N° CERTA-2011-ACT-009

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2011-09

Gestion du document

Référence	CERTA-2011-ACT-009
Titre	Bulletin d'actualité 2011-09
Date de la première version	04 mars 2011
Date de la dernière version	–
Source(s)	–
Pièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

Le bulletin d'actualité est disponible dans son intégralité et au format PDF à l'adresse suivante :
http://www.certa.ssi.gouv.fr/site/CERTA-2011-ACT-009.pdf
Un extrait du bulletin, ne reprenant que les articles de la semaine, se trouve en HTML à l'adresse suivante :
http://www.certa.ssi.gouv.fr/site/CERTA-2011-ACT-009/

1 Compromission d'un site sous Joomla!

Le CERTA a traité cette semaine le cas d'une compromission de site fonctionnant avec *Joomla!*. Les incidents de ce type sont fréquents, et découlent généralement de l'exploitation d'une vulnérabilité dans un module optionnel. Dans le cas abordé cette semaine, il s'agit d'une autre méthode d'attaque : les attaques par dictionnaire. Ces dernières se caractérisent dans les journaux par des traces du type :

```
<IP attaquant> - - [01/Mar/2011:02:41:23 +0100] "POST /administrator/index.php HTTP/1.1"
200 4646 - - -
<IP attaquant> - - [01/Mar/2011:02:41:23 +0100] "POST /administrator/index.php HTTP/1.1"
200 4646 - - -
<IP attaquant> - - [01/Mar/2011:02:41:24 +0100] "POST /administrator/index.php HTTP/1.1"
200 4646 - - -
...
<IP attaquant> - - [01/Mar/2011:02:41:25 +0100] "POST /administrator/index.php HTTP/1.1"
303 5 - - -
<IP attaquant> - - [01/Mar/2011:02:41:26 +0100] "GET /administrator/index.php HTTP/1.1"
200 22374 - - -
```

Une fois connecté au panneau d'administration, l'attaquant a accès à des scripts permettant le dépôt de fichiers. Il lui devient notamment possible d'installer une porte dérobée sous la forme d'un interpréteur de commandes écrit en `PHP`.

Dans l'incident traité, l'attaquant a, après avoir déposé sa porte dérobée, tenté d'étendre la compromission à tout le serveur en exploitant plusieurs vulnérabilités du noyau Linux.

Recommandations

Le CERTA recommande à tous les utilisateurs de services informatiques de lire la note d'information CERTA-2005-INF-001 relative aux mots de passe (voir la section « Liens utiles »). Il est, de plus, conseillé aux administrateurs de site Web de lire régulièrement leurs journaux d'accès, et de vérifier que seuls des administrateurs légitimes naviguent sur les pages des différents panneaux d'administration. Enfin, il est recommandé de restreindre l'accès aux pages d'administration (par exemple à des adresses IP spécifiques).

2 NoScript à l'origine de requêtes « étranges »

NoScript est un module complémentaire pour navigateurs Web (*Mozilla FireFox*, *SeaMonkey* et autres navigateurs basés sur *Mozilla*) qui ajoute des fonctionnalités de sécurité.

Il permet par exemple d'établir des listes blanches de domaines pour lesquels l'exécution de code JavaScript ou Adobe Flash sont autorisés. Il intègre également des mécanismes de détection d'exploitation de failles de type injection de code indirecte à distance, ou « XSS ».

Un autre élément utilisé par NoScript est *ABE* pour *Application Boundary Enforcer*. Il se propose d'améliorer les mécanismes de défense contre les injections de code indirectes, en instaurant dans le navigateur des protections supplémentaires que l'utilisateur peut configurer. Celui-ci va pouvoir par exemple interdire toute requête à des serveurs Web situés dans le réseau local du poste, qui proviennent d'un site externe à ce dernier.

L'intérêt est de pouvoir bloquer par exemple des scripts qui tenteraient de scanner le réseau interne ou de réaliser des injections de requêtes illégitimes par rebond (*Cross-Site Request Forgery*) sur ces derniers.

```
# LOCAL représente les adresses IP locales.
Site LOCAL              # Pour les sites sur des adresses locales
Accept from LOCAL       # on accepte seulement les requêtes provenant de celles-ci
deny                    # et on rejette toutes les autres
```

On évite également ainsi qu'un script installé sur un site malveillant tente de se connecter à l'interface administrateur d'un routeur domestique, celle-ci utilisant souvent des identifiants de connexion par défaut, ou très faibles, ou encore possèdant des vulnérabilités.

Le mot-clé *LOCAL* regroupait initialement les adresses locales, par exemple 127.0.0.1 et le réseau 192.168.0.0/24. Il est facile de connaître le réseau local du poste, en demandant son adresse IP. Or, il a été présenté en été 2010, que bon nombre des routeurs domestiques étaient capables de répondre à une requête adressée à leur adresse IP publique mais provenant de l'interface interne. Un script malveillant peut donc tenter de communiquer avec le routeur depuis un poste sur le réseau interne en contournant les protections présentées ci-dessus.

Depuis la version 2.0rc5 de *NoScript*, une nouvelle fonctionnalité à été ajoutée à ABE, relative à la règle concernant le réseau local décrite ci-dessus. Pour interdire ce dernier type d'attaque, le module effectue une requête anonymisée au site https://secure.informaction.com/ipecho/ afin de déterminer l'adresse publique utilisée par le routeur, et l'ajouter à la liste des adresses représentées par le mot-clé *LOCAL*. Tous les postes utilisant l'extension *NoScript* avec le module ABE activé vont donc effectuer quotidiennement des requêtes à cette adresse.

Comme il arrive que certains routeurs changent d'IP publique très régulièrement, il convient de faire cette vérification plus fréquemment. Toutefois, pour éviter de surcharger le serveur à l'adresse secure.informaction.com par un grand nombre de requêtes, les développeurs de *NoScript* ont décidé de mettre en place un système de cache.

Par intervalles de quelques minutes, une requête est envoyée à l'adresse IP publique précédemment détectée, et une signature de la réponse est enregistrée. Si cette signature est modifiée, *NoScript* détecte que l'adresse publique utilisée par le routeur a changé, et effectue une nouvelle connexion à l'adresse secure.informaction.com pour trouver la nouvelle adresse IP publique.

Un routeur reliant un parc comprenant des postes d'utilisateurs, dont le navigateur Web utilise l'extension *NoScript* en version 2.0rc5 ou postérieure, va donc voir une augmentation significative de requêtes HTTP à destination de son adresse IP publique, sur son interface de réseau local.

Si un serveur Web est installé sur le routeur et configuré pour écouter sur son interface interne, celui-ci enregistrera dans ses journaux des requêtes du type :

```
XX.YY.ZZ.TT   "GET / HTTP/1.1" 200 370 "-" "Mozilla/5.0 (ABE, http://noscript.net/abe/wan)"
```

avec XX.YY.ZZ.TT, l'adresse IP publique du routeur/serveur.

Pour demander à *NoScript* de ne plus effectuer ces requêtes, il suffit de décocher l'option WAN IP $\in$ LOCAL dans la rubrique *NoScript Option* $\rightarrow$ *Advanced* $\rightarrow$ *ABE*. Attention, car dans ce cas, l'adresse IP publique ne sera alors plus considérée comme une adresse locale, et le routeur sera de nouveau exposé aux attaques indiquées ci-dessus.

Documentation

- Site officiel de l'extension NoScript :
  http://noscript.net
- Présentation d'ABE :
  http://noscript.net/abe/
- Language de la configuration d'ABE :
  http://noscript.net/abe/abe_rules.pdf
- Description de la détection de l'adresse IP publique :
  http://hackademix.net/2010/07/28/abe-patrols-the-routes-to-your-routers/
- Fil de discussion sur l'origine du trafic Web sur le routeur :
  http://forums.informaction.com/viewtopic.php?f=7&t=4743
- Note d'information CERTA sur les vulnérabilités de type injection de code indirecte, ou « XSS » CERTA-2002-INF-001 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-001/
- Note d'information CERTA sur les vulnérabilités de type injection de requête illégitime par rebond, ou « CSRF » CERTA-2008-INF-003 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-INF-003/

3 Liens utiles

- Mémento sur les virus :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-002/
- Note d'information du CERTA sur l'acquisition de correctifs :
  http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-004/
- Note d'information du CERTA sur les systèmes obsolètes :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-003/
- Note d'information du CERTA sur les bonnes pratiques concernant l'hébergement mutualisé :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005/
- Note d'information du CERTA sur les mots de passe :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/
- Note d'information sur la terminologie d'usage au CERTA :
  http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-002/
- Note d'information du CERTA sur les enjeux de sécurité liés à une migration vers IPv6 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-004/
- Unix security checklist version 2.0 du 8 octobre 2001 (Publication du CERT australien) :
  http://www.auscert.org.au/render.html?it=1937
- Note d'information du CERTA sur les risques associés aux clés USB :
  http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-006/
- Note d'information du CERTA sur les outils d'indexation et de recherche :
  http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-009/
- Note d'information du CERTA sur la gestion des noms de domaine :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-001/
- Note d'information du CERTA sur le bon usage de PHP :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-002/

4 Rappel des avis émis

Dans la période du 25 février au 03 mars 2011, le CERTA a émis les avis suivants :

- CERTA-2011-AVI-111 : Vulnérabilité dans F-Secure Policy Manager
- CERTA-2011-AVI-112 : Multiples vulnérabilités dans SumatraPDF
- CERTA-2011-AVI-113 : Multiples vulnérabilités dans MuPDF
- CERTA-2011-AVI-114 : Vulnérabilité dans Citrix XenApp et XenDesktop
- CERTA-2011-AVI-115 : Vulnérabilité dans RT
- CERTA-2011-AVI-116 : Vulnérabilité dans Citrix Secure Gateway
- CERTA-2011-AVI-117 : Vulnérabilité dans IBM Lotus Connections
- CERTA-2011-AVI-118 : Vulnérabilité dans IBM Tivoli Common Reporting
- CERTA-2011-AVI-119 : Vulnérabilité dans Foxit Reader
- CERTA-2011-AVI-120 : Vulnérabilité dans Samba
- CERTA-2011-AVI-121 : Vulnérabilité dans Avahi
- CERTA-2011-AVI-122 : Vulnérabilité dans Sybase Afaria Data Security Manager
- CERTA-2011-AVI-123 : Vulnérabilité dans HP Web Jetadmin
- CERTA-2011-AVI-124 : Vulnérabilité dans PEAR
- CERTA-2011-AVI-125 : Multiples vulnérabilités dans Wireshark
- CERTA-2011-AVI-126 : Multiples vulnérabilités dans Google Chrome
- CERTA-2011-AVI-127 : Multiples vulnérabilités dans les produits Mozilla
- CERTA-2011-AVI-128 : Vulnérabilité dans Alcatel OmniPCX Enterprise
- CERTA-2011-AVI-129 : Vulnérabilités dans libpango
- CERTA-2011-AVI-130 : Vulnérabilité dans Alcatel OmniVista

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

- CERTA-2011-AVI-079-004 : Vulnérabilité dans plusieurs implémentations de Java (ajout de la référence au bulletin de sécurité HP c02729756)
- CERTA-2011-AVI-103-001 : Vulnérabilité dans ISC Bind (révision des versions affectées, ajout des références Novell (Suse) et Ubuntu)

5 Actions suggérées

5.1 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.

5.2 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.

5.3 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.

5.4 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.

5.5 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.

5.6 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.

5.7 Former et sensibiliser les utilisateurs

La sécurité d'un système d'information doit reposer sur une approche de défense en profondeur. Cela signifie, entre autres choses, que l'utilisateur est partie prenante de la sécurité. Sa vigilance, son niveau de formation et de sensibilisation participent à la sécurité du système. C'est pourquoi il est essentiel de prévoir des séances de formation et de sensibilisation des utilisateurs, acteurs de la sécurité. Pour vous aider dans ces actions, l'ANSSI dispose d'un centre de formation :

http://www.ssi.gouv.fr/site_rubrique62.html

6 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.

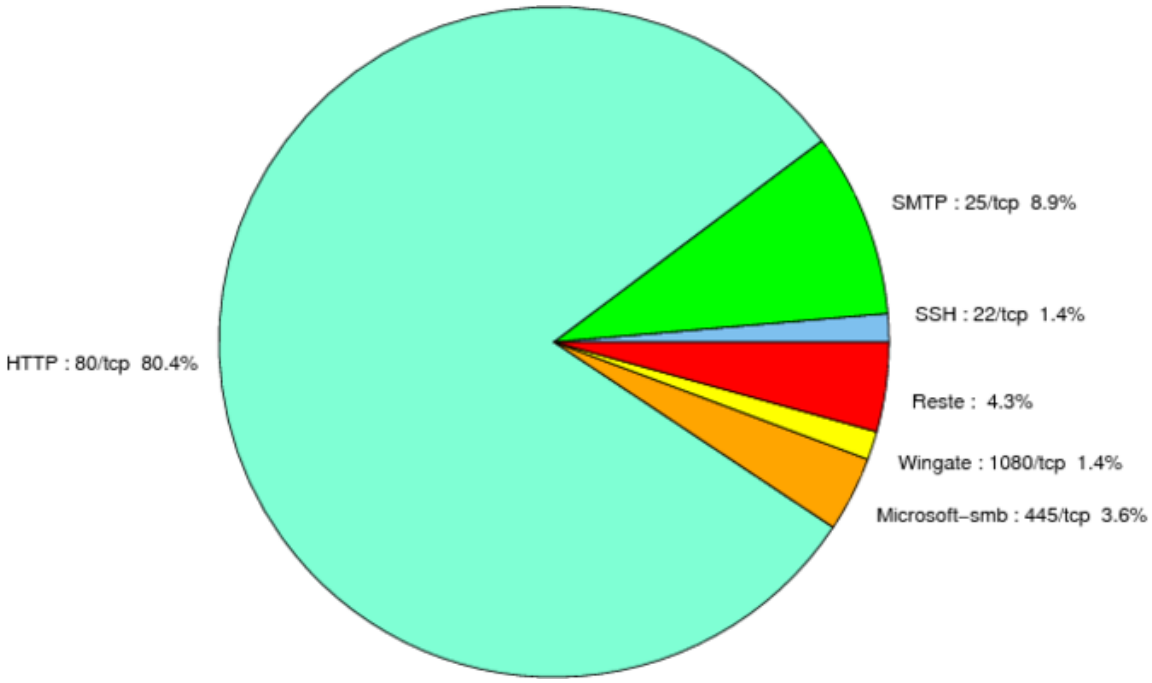

FIG. 1: Répartition relative des ports pour la semaine du 25 février au 03 mars 2011

port	pourcentage
80/tcp	89.94
25/tcp	8.89
445/tcp	3.62
1080/tcp	1.38
23/tcp	1
3389/tcp	0.97
143/tcp	0.5
135/tcp	0.47
3306/tcp	0.19
3128/tcp	0.16
4899/tcp	0.14
2967/tcp	0.07

TAB. 2: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

04 mars 2011 version initiale.