

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2011-14

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-2011-ACT-014>

Gestion du document

Référence	CERTA-2011-ACT-014
Titre	Bulletin d'actualité 2011-14
Date de la première version	08 avril 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-014.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-014/>

1 Vulnérabilité dans certaines implémentations de IPComp

Le protocole d'encapsulation *IPComp* (décrit dans la RFC3173) est utilisé pour compresser la charge utile transportée par un datagramme IP.

Une faille dans les implémentations de piles IPComp provenant de NetBSD et du projet KAME permet à une personne malveillante de réaliser un déni de service via un débordement de la pile du noyau. Il semble également possible d'exploiter dans certains cas cette vulnérabilité pour exécuter du code arbitraire à distance.

Cette implémentation étant reprise dans de très nombreux produits, il convient de vérifier pour chacun d'entre eux si la pile IPComp est activée, et si celle-ci est vulnérable.

Les distributions NetBSD et FreeBSD ont déjà rendu public des correctifs pour leur noyau respectif sous la forme de modification du code source.

Le CERTA recommande aux utilisateurs de produits embarquant un noyau BSD de filtrer le protocole IPComp si celui-ci n'est pas nécessaire et de vérifier avec le fabricant la présence ou non de cette vulnérabilité.

Documentation

– RFC3173 :

- <http://datatracker.ietf.org/doc/rfc3173/>
- Projet KAME :
<http://www.kame.net>
- Mise à jour du noyau NetBSD :
<http://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2011-004.txt.asc>
- Mise à jour du noyau FreeBSD :
<http://svn.freebsd.org/viewvc/base?view=revision&revision=220247>

2 Attaques par contournement, scénario qui se généralise

Le CERTA constate des intrusions indirectes. Généralisation d'un phénomène, ou simplement meilleure observation de celui-ci, la question mérite d'être posée. Toutefois les nombreuses attaques directes militent pour la première hypothèse.

Dans un billet sur son blog, la société RSA décrit le déroulement de l'attaque qui a permis à des intrus de voler des informations sensibles liées à l'un de ses produits, le *token* SecurID. La description correspond au schéma auquel des correspondants du CERTA sont confrontés. L'attaque se fait par approche progressive vers les données convoitées. Le cas de RSA sert au jalonnement de la description.

Sur les processus critiques visés, les utilisateurs sont probablement sensibilisés et des outils de protection sont mis en place. L'attaquant cherche un point plus faible, un utilisateur sans rôle particulier.

L'entrée dans le système d'information utilise l'ingénierie sociale pour inciter à ouvrir un courriel piégé exploitant une vulnérabilité non corrigée, ou tout juste corrigée, avec l'espoir que le déploiement des correctifs aura été assez lent pour laisser des postes vulnérables. Le piège est généralement personnalisé pour ne pas être détecté par les outils de protection (antivirus, IDS...). Un autre vecteur peut être une clef USB déposée près de l'entrée de la société ou de l'organisme cible.

Dans le cas de RSA des utilisateurs ordinaires ont reçu, en deux vagues, des courriels intitulés « 2011 Recrutement Plan », (prévision de recrutement 2011), avec un fichier excel joint, lequel embarquait un objet Flash exploitant la vulnérabilité CVE-2011-0609, corrigée par Adobe le 21 mars 2011. Le piège a consisté en l'installation d'une version du code malveillant PoisonIvy. Il a suffi d'un seul utilisateur ouvrant la pièce jointe pour ouvrir les portes aux intrus.

Une fois dans la place, comme à Troie, l'agresseur peut sévir. Le schéma classique est d'installer un logiciel malveillant capable de prendre des ordres ou de télécharger une charge active. Les défenses périmétriques étant généralement restrictives, ces ordres ou ces téléchargements utilisent un canal plus probablement ouvert. Il s'agit souvent du protocole HTTP ou HTTPS. Il est donc important de restreindre et de surveiller les flux sortants (source/destination, volume, horaire...). Un attaquant plus subtil utilisera des canaux cachés.

Il faut déterminer la localisation de la tête de pont par rapport à la cible finale. Cette phase passe par une cartographie et un relevé technique sur le SI (plan d'adressage, version des systèmes...).

L'agresseur peut également préparer des accès (toujours illégitimes) de secours anticipant la découverte de l'intrusion initiale. Il peut également préparer des outils de collecte et de sortie des données pillées.

Selon les privilèges de l'utilisateur qui s'est fait berné et les protections des informations ciblées, l'attaquant utilisera les droits de ce dernier ou devra se servir d'un programme malveillant qui permettra à son cheval de Troie d'acquérir des droits d'administration.

Ces agissements rencontrés dans des attaques récentes montrent des attaquants déterminés et motivés. La réaction doit être globale et non limitée au déploiement de mesures techniques non administrées.

2.1 Recommandations

La défense en profondeur, combinant les aspects organisationnels, humains et techniques, demeure un principe de base face à ces attaques. Il en résulte des recommandations complémentaires :

- élaborer une politique de sécurité des SI, connue de tous et qui reprendra des points ci-dessous ;
- sensibiliser *tous* les utilisateurs à la SSI ;
- cloisonner le système d'information ;
- appliquer la politique des moindres privilèges, par exemple en limitant les comptes d'administration des postes et des domaines en nombre et dans leur usage, et en gérant de manière restrictive les droits d'accès sur les ressources ;

- inclure la SSI dans l’informatisation des processus métier et dans le cycle de vie des applications ;
- mettre en place des procédures de déploiement des mises à jour et des palliatifs ;
- journaliser les accès réseau et les transactions, et les analyser (idéalement en continu) ;
- prévoir des procédures en cas d’incident et de suspicion ;
- utiliser des mots de passe forts ou des moyens d’authentification renforcée ;
- répéter les mises en garde sur les supports amovibles (clefs USB, ordiphones et autres) ;
- réévaluer les risques et amender la politique de sécurité.

2.2 Documentation

- Anatomy of an attack :
<http://blogs.rsa.com/rivner/anatomy-of-an-attack/>
- Chronique d’un incident ordinaire :
<http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-003/index.html>
- Les systèmes et logiciels obsolètes :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-003/index.html>
- Les mots de passe :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/index.html>

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 01 au 07 avril 2011, le CERTA a émis les avis suivants :

- CERTA-2011-AVI-182 : Vulnérabilité dans Juniper IVE
- CERTA-2011-AVI-183 : Vulnérabilité dans Claroline
- CERTA-2011-AVI-184 : Vulnérabilité dans IBM AIX

- CERTA-2011-AVI-185 : Multiples vulnérabilités dans HP Operations for Unix
- CERTA-2011-AVI-186 : Vulnérabilité dans HP Network Node Manager i
- CERTA-2011-AVI-187 : Vulnérabilité dans Joomla!
- CERTA-2011-AVI-188 : Vulnérabilité dans Novell File Reporter
- CERTA-2011-AVI-189 : Vulnérabilités dans logrotate
- CERTA-2011-AVI-190 : Vulnérabilité dans le client DHCP ISC
- CERTA-2011-AVI-191 : Vulnérabilité dans xrdp (XOrg)
- CERTA-2011-AVI-192 : Vulnérabilités dans WordPress
- CERTA-2011-AVI-193 : Vulnérabilité dans la glibc
- CERTA-2011-AVI-194 : Vulnérabilité dans Oracle Solaris

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

- CERTA-2011-AVI-079-005 : Vulnérabilité dans plusieurs implémentations de Java (ajout de la référence au bulletin IBM swg21474615 Tivoli Directory Server)
- CERTA-2011-AVI-164-001 : Vulnérabilité dans Xpdf sur Linux (ajout de la référence CVE CVE-2011-1554)

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 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.

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 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.

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.

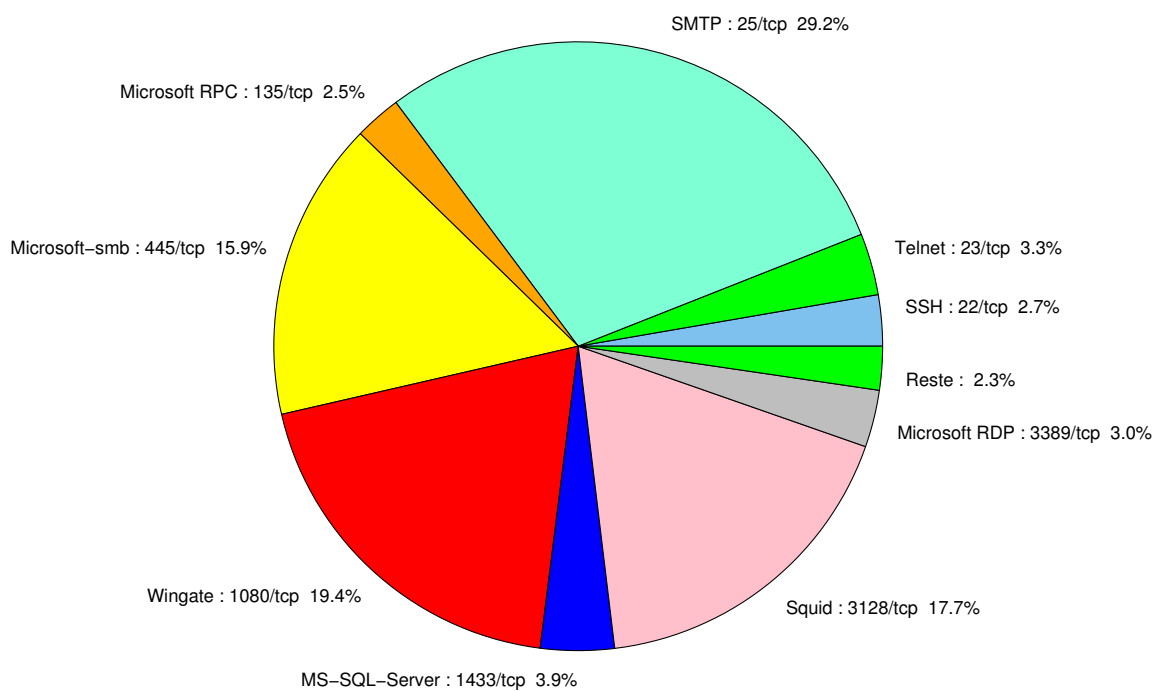


FIG. 1: Répartition relative des ports pour la semaine du 01 au 07 avril 2011

port	pourcentage
25/tcp	29.23
1080/tcp	19.4
3128/tcp	17.73
445/tcp	15.89
1433/tcp	3.91
23/tcp	3.27
3389/tcp	3.03
22/tcp	2.71
135/tcp	2.47
80/tcp	2.31
3306/tcp	0.87
4899/tcp	0.55
2967/tcp	0.47
21/tcp	0.39

TAB. 2: Paquets rejetés

Liste des tableaux

1	Gestion du document	1
2	Paquets rejetés	6

Gestion détaillée du document

08 avril 2011 version initiale.