Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 18 mai 2012
N° CERTA-2012-ACT-020

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2012-20

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-2012-ACT-020`

Gestion du document

Référence	CERTA-2012-ACT-020
Titre	Bulletin d'actualité 2012-20
Date de la première version	18 mai 2012
Date de la dernière version	–
Source	–
Pièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

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

1 RFC 6598 et adresses IPv4 réservées

L'espace d'adressage IPv4 est presque épuisé. En attente du déploiement complet d'IPv6, les fournisseurs d'accès doivent répondre à la demande croissante d'adresses IPv4. Jusqu'à présent, cela se faisait essentiellement en s'appuyant sur les adresses IP réservées par le standard RFC 1918. En avril 2012 a été publié le RFC 6598, relatif à la réservation du préfixe IPv4 100.64.0.0/10. Ce bloc d'adresses est appelé *Shared Address Space*. Son fonctionnement est assez similaire à l'espace d'adressage privé défini par le RFC 1918, mais il est réservé aux fournisseurs d'accès. Il s'appuie sur des périphériques CGN (*Carrier-Grade NAT*).

D'un point de vue de la sécurité, l'arrivée de ces nouvelles adresses IP n'est pas forcément simple à gérer. En effet, le bloc d'adresses 100.64.0.0/10 devrait être filtré, sauf si le fournisseur d'accès l'utilise. Dans ce dernier cas, tout trafic ayant pour source une adresse IP dans le bloc 100.64.0.0/10 provient théoriquement du fournisseur d'accès (ou d'un de ses clients), à condition que celui-ci filtre correctement en bordure.

Le tableau des adresses IP spéciales, défini dans le RFC 5735, est donc complété de la façon suivante :

Bloc d'adressage	RFC	Routable sur l'Internet
0.0.0.0/8	RFC 1122	non
10.0.0.0/8	RFC 1918	non
100.64.0.0/10	RFC 6598	non (sauf chez le FAI)
127.0.0.0/8	RFC 1122	non
169.254.0.0/16	RFC 3927	non
172.16.0.0/12	RFC 1918	non
192.0.2.0/24	RFC 5737	non
192.88.99.0/24	RFC 3068	oui (routeurs 6to4)
192.168.0.0/16	RFC 1918	non
198.18.0.0/15	RFC 2544	non
198.51.100.0/24	RFC 5737	non
203.0.113.0/24	RFC 5737	non
224.0.0.0/4	RFC 3171	oui (multicast)
240.0.0.0/4	RFC 1700	non (réservé pour un usage futur)

Documentation

- RFC 6598 :
  http://tools.ietf.org/html/rfc6598
- RFC 5735 :
  http://tools.ietf.org/html/rfc5735

2 Support Adobe

Le 08 mai 2012, des vulnérabilités affectant les logiciels *Adobe* avaient été publiées. Celles-ci touchaient les versions CS5 et CS6 de plusieurs produits, mais le correctif apporté par *Abode* visait la version CS6, laissant la version CS5 vulnérable. La seule solution proposée était de passer à la version CS6, payante, provoquant des réactions d'utilisateurs.

Le 11 mai 2012, une mise à jour des bulletins a été réalisée spécifiant dans l'historique du bulletin un « ajout d'informations pour la mise à jour de la suite CS5.x ». Il s'agit de la publication prévue de correctifs pour cette version. Il faut donc noter que la suite CS5 est, pour l'instant, supportée par *Adobe*.

3 Rappel des avis émis

Dans la période du 11 au 17 mai 2012, le CERTA a émis les publications suivantes :

- CERTA-2012-AVI-274 : Multiples vulnérabilités dans EMC Documentum Information Rights Management
- CERTA-2012-AVI-275 : Vulnérabilité dans Opera
- CERTA-2012-AVI-276 : Vulnérabilité dans IBM Rational ClearQuest
- CERTA-2012-AVI-277 : Vulnérabilité dans OpenSSL
- CERTA-2012-AVI-278 : Vulnérabilités dans Sympa
- CERTA-2012-AVI-279 : Multiples vulnérabilités dans Google Chrome
- CERTA-2012-AVI-280 : Vulnérabilités dans SPIP
- CERTA-2012-AVI-281 : Vulnérabilité dans Socat

4 Actions suggérées

4.1 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.

4.2 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.

4.3 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.

4.4 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.

4.5 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.

4.6 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.

4.7 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

Gestion détaillée du document

18 mai 2012 version initiale.