Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 20 avril 2012
N° CERTA-2012-ACT-016

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2012-16

Gestion du document

Référence	CERTA-2012-ACT-016
Titre	Bulletin d'actualité 2012-16
Date de la première version	20 avril 2012
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.

1 Réduction des risques liés à des vulnérabilités dans les applications fonctionnant sous Windows

EMET (Enhanced Mitigation Experience Toolkit) est un outil développé par Microsoft permettant, dans certains cas, de rendre plus difficile l'exploitation d'une vulnérabilité dans un logiciel fonctionnant sous Windows. Il peut être utilisé à partir de *Windows XP*. Il greffe quatre protections aux logiciels que vous souhaitez protéger :

- protection appelée *ASLR* (*address space layout randomization*) qui consiste en un ajout de 8 bits d'entropie dans l'adresse lors de l'allocation de certaines zones mémoire ;
- ajout d'un mécanisme empêchant l'exploitation de vulnérabilités par les *shellcodes* les plus courants (*EAF - EAT Access Filtering*) ;
- activation automatique de la protection de « débordement de tampon en pile » dite *SEHOP* ;
- protection contre les attaques de type *heap spraying*, très couramment utilisées lors des attaques sur les navigateurs Internet ;
- activation automatique de la protection dite *DEP* (*Data Execution Prevention*).

Cette suite de protections rend un grand nombre d'outils d'attaque inopérants, comme *Microsoft* l'a souligné en citant des exemples d'utilisation d'*EMET* pour limiter l'impact de vulnérabilités sur certaines versions de produits *Adobe*.

Le CERTA recommande d'utiliser cet outil sur les systèmes les plus exposés aux attaques extérieures, en complément d'une architecture de défense en profondeur.

Documentation :

- Trousse à outils EMET :
  http://support.microsoft.com/kb/2458544/fr
- Téléchargement d'EMET :
  http://www.microsoft.com/download/en/details.aspx?id=1677
- Exemples d'utilisation d'EMET :
  http://blogs.technet.com/b/srd/archive/2010/09/1 0/use-emet-2-0-to-block-the-adobe-0-day-exploit.aspx
  http://blogs.technet.com/b/srd/archive/201 1/03/17/blocking-exploit-attempts-of-the-recent-flash-0-day.aspx

2 Filtrage de messagerie : à utiliser avec modération

À l'instar d'autres émetteurs légitimes, le CERTA est régulièrement confronté à la non-remise silencieuse de ses courriels à destination de ses correspondants. Ce phénomène regrettable s'explique par le contenu de certains courriels, dans lesquels figurent des détails techniques utiles aux destinataires. Ces détails peuvent être des adresses réticulaires (URL) malveillantes ou prendre des formes plus explicites d'exploitation de vulnérabilité (XSS, injection SQL, LFI, RFI, ...). Ces contenus considérés comme malveillants sont éliminés par des filtres de messagerie.

La transmission d'adresses réticulaires malveillantes n'est pas la seule source de rejet. Par exemple, le CERTA a été récemment informé que certains de ses avis sont régulièrement qualifiés de pourriels et traités comme tels. L'utilisation de nombreuses adresses réticulaires dans la section *Documentation* des avis du CERTA peut être pénalisante lors du traitement par des filtres anti-spam. Parmi les critères utilisés pour différencier les courriels légitimes des pourriels, certains filtres s'appuient, entre autres, sur le nombre d'adresses réticulaires contenues dans les messages.

Il n'existe pas de solution miracle à ce problème. En effet, dans notre exemple :

- mettre l'adresse d'expéditeur du CERTA (certa-svp@certa.ssi.gouv.fr) en liste blanche pour assurer la réception de ces courriels risque d'autoriser également la réception de pourriels usurpant cette adresse ;
- mettre l'adresse IP du serveur SMTP du CERTA en liste blanche présente le risque de laisser entrer des courriels malveillants si ce serveur venait à être compromis.

Dans tous les cas, la détermination du caractère désirable ou indésirable d'un courriel est un art complexe. Il faut donc régler et adapter régulièrement les filtres de messagerie (IPS, passerelles, serveurs, poste). Ce travail de personnalisation des filtres doit prendre en compte des risques assumés : celui de la réception de courriels indésirables, éventuellement marqués, ou celui de la non-réception de courriels légitimes.

Documentation

- Note d'information du CERTA - *Limiter l'impact du SPAM* :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-004/index.html
- Note d'information du CERTA - *Mesures de prévention relatives à la messagerie* :
  http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-002/index.html

3 Rappel des avis émis

Dans la période du 13 au 19 avril 2012, le CERTA a émis les publications suivantes :

- CERTA-2012-AVI-212 : Vulnérabilité dans WICD
- CERTA-2012-AVI-213 : Vulnérabilité dans nginx
- CERTA-2012-AVI-214 : Multiples vulnérabilités dans Invision Power Board
- CERTA-2012-AVI-215 : Vulnérabilité dans VMware
- CERTA-2012-AVI-216 : Multiples vulnérabilités dans RealPlayer
- CERTA-2012-AVI-217 : Vulnérabilités dans IBM Tivoli
- CERTA-2012-AVI-218 : Multiples vulnérabilités dans HP System Management Homepage
- CERTA-2012-AVI-219 : Multiples vulnérabilités dans HP OpenVMS
- CERTA-2012-AVI-220 : Multiples vulnérabilités dans Oracle

– CERTA-2012-AVI-221 : Vulnérabilité dans HP Onboard Administrator
– CERTA-2012-AVI-222 : Vulnérabilité dans Apache

Durant la même période, les publications suivantes ont été mises à jour :

– CERTA-2012-ALE-002-001 : Vulnérabilité dans Windows RDP (explicitation du correctif éditeur comme solution)
– CERTA-2012-AVI-085-002 : Multiples vulnérabilités dans Oracle Java (ajout des correctifs IBM)

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

20 avril 2012 version initiale.