Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 03 août 2012
N° CERTA-2012-ACT-031

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : CERTA-2012-ACT-031

Gestion du document

Référence	CERTA-2012-ACT-031
Titre	CERTA-2012-ACT-031
Date de la première version	03 août 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.

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-2012-ACT-031.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-2012-ACT-031/

1 ModSecurity pour IIS

L'extension ModSecurity, qui permet de réaliser un serveur mandataire filtrant (*reverse-proxy*), est désormais disponible pour le serveur Web Microsoft IIS. Cette extension est pour l'instant uniquement disponible en version de test (*release candidate*), le CERTA ne recommande donc pas sa mise en place sur des réseaux de production mais il peut être intéressant de la déployer sur un réseau de test. ModSecurity est compatible avec les versions 7 et suivantes de IIS.

ModSecurity permet de mettre en place des règles de filtrage afin de protéger les sites Web contre certaines attaques. Il est fourni par défaut avec un jeu de règles permettant de bloquer les attaques les plus communes, en mode liste noire.

Il est essentiel de qualifier la mise en place de ModSecurity, afin de ne pas bloquer d'éventuels faux-positifs. De plus, il est recommandé de déployer ModSecurity en mode liste blanche, en configurant l'ensemble des requêtes nécessaires au fonctionnement du site.

Comme tout produit de sécurité, il est recommandé d'activer les journaux d'événements et de surveiller les traces ainsi produites.

Documentation

– Annonce de la sortie de ModSecurity pour IIS sur le blog Security Research & Defense de Microsoft
http://blogs.technet.com/b/srd/archive/2012/07/26/announcing-the-availability-of-modsecurity-extension-for-iis.aspx

2 Sortie d'une version de test de EMET 3.5

Le 24 juillet *Microsoft* a publié les travaux ayant remporté le concours *BlueHat*. Il s'agit d'un ajout aux fonctionnalités de EMET (*Enhanced Mitigation Experience Toolkit*), un outil destiné à rendre plus difficile l'exploitation d'une vulnérabilité dans un logiciel fonctionnant sous Windows. L'auteur s'est basé sur le fait qu'aujourd'hui la majorité des exploits stables utilise le *Return Oriented Programming*. Cette méthode est employée pour contourner de nombreuses protections comme la prévention d'exécution des données (DEP) qui permet de rendre non exécutable certaines zones mémoires.

Cinq méthodes de détection et de prévention ont été ajoutées à EMET. Elles se basent principalement sur la surveillance à des fonctions critiques comme *GetProcAddress* ou *WinExec* afin de détecter des incohérences de la pile et des futures instructions à exécuter. Ainsi la majorité des exploits actuellement utilisés est bloquée par ce système. Ces mesures apportent une protection supplémentaire mais elles ne permettent pas de garantir que l'exploitation d'une vulnérabilité soit complétement bloquée. Cet outil contribue donc à une démarche de défense en profondeur du système.

Ce produit étant pour l'instant disponible uniquement en version de test, le CERTA ne recommande pas son intégration dans un système en production. Il peut cependant être pertinent de le déployer sur un environnement de test afin de qualifier son impact sur les applications métier.

Documentation

– Présentation d'EMET 3.5 sur le blog Security Research & Defense de Microsoft :
http://blogs.technet.com/b/srd/archive/2012/07/24/emet-3-5-tech-preview-leverages-security-mitigations-from-the-bluehat-prize.aspx

3 Rappel des avis émis

Dans la période du 27 juillet 2012 au 02 aout 2012, le CERTA a émis les publications suivantes :

– CERTA-2012-AVI-407 : Vulnérabilités dans IBM SONAS
– CERTA-2012-AVI-408 : Vulnérabilités dans Bugzilla
– CERTA-2012-AVI-409 : Vulnérabilité dans Ruby on Rails
– CERTA-2012-AVI-410 : Vulnérabilité dans IBM AIX
– CERTA-2012-AVI-411 : Vulnérabilité dans IBM WebSphere
– CERTA-2012-AVI-412 : Vulnérabilités dans Django
– CERTA-2012-AVI-413 : Vulnérabilité dans SIMATIC S7-400 CPU
– CERTA-2012-AVI-414 : Vulnérabilités dans IBM Rational Directory Server
– CERTA-2012-AVI-415 : Vulnérabilités dans Google Chrome
– CERTA-2012-AVI-416 : Vulnérabilités dans Kerberos

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 CERTA recommande l'application des correctifs de sécurité.

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

03 août 2012 version initiale.