Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 24 août 2012
N° CERTA-2012-ACT-034

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : CERTA-2012-ACT-034

Gestion du document

Référence	CERTA-2012-ACT-034
Titre	CERTA-2012-ACT-034
Date de la première version	24 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-034.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-034/

1 Compromissions c3284d

Depuis juin 2012, de nombreux sites Web font l'objet de compromissions répétées, qui se manifestent par l'ajout de code *javascript* provoquant des redirections vers des sites malveillants. L'ajout de ce code *javascript* peut se faire dans les fichiers .php, .html ou .htaccess. Quel que soit le type du fichier modifié, le code *javascript* contient la chaîne de caractères *c3284d*.

Le CERTA a déjà été amené à traiter plusieurs de ces compromissions. Dans certains cas, lors d'une navigation sur le site Web compromis, le code *javascript* s'affiche au lieu de s'exécuter. Dans tous les cas analysés par le CERTA, les attaquants ont utilisé des identifiants FTP légitimes. Les connexions FTP ont lieu régulièrement (presque tous les jours), depuis des adresses IP différentes. À chacune de ces connexions, il y a dépôt puis suppression d'un ou plusieurs fichiers composés d'une chaîne de huit caractères et de l'extension .gif.

Le CERTA recommande :

– de rechercher l'éventuelle présence de la chaîne de caractères *c3284d* dans les arborescences des sites Web ;
– de vérifier dans les journaux FTP la présence de connexions illégitimes ;
– de filtrer les accès FTP ;
– de vérifier l'intégrité des postes ayant été redirigés après navigation sur un site Web compromis.

2 Publication d'un avis de sécurité Microsoft sur la vulnérabilité MS-CHAPv2

Le CERTA a évoqué dans le bulletin d'actualité CERTA-2012-ACT-032 les dangers liés l'utilisation du protocole d'authentification MS-CHAPv2. Pour rappel, un nouvel outil visant MS-CHAPv2 a récemment été publié. Celui-ci permet un attaquant diposant d'un défi-réponse d'obtenir le secret d'authentification, théoriquement protégé par le protocole. Microsoft a publié cette semaine un avis de sécurité qui rappelle que les VPN basés sur PPTP sont affectés et donne des recommandations pour contourner ces vulnrabilités inhérentes au protocole. Le CERTA recommande d'étudier les solutions proposées pour les appliquer, après une évaluation d'impact.

Références

- Bulletin d'actualité CERTA-2012-ACT-032
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-ACT-032/index.html
- Avis de sécurité Microsoft (2743314)
  http://technet.microsoft.com/fr-fr/security/advisory/2743314
  http://technet.microsoft.com/en-us/security/advisory/2743314
- Weaknesses in MS-CHAPv2 authentication
  http://blogs.technet.com/b/srd/archive/2012/08/20/weaknesses-in-ms-chapv2-authentication.aspx

3 Rappel des avis émis

Dans la période du 17 août 2012 au 23 août 2012, le CERTA a émis les publications suivantes :

- CERTA-2012-AVI-444 : Vulnérabilité dans Cisco IOS XR
- CERTA-2012-AVI-445 : Vulnérabilité dans Adobe Flash Player
- CERTA-2012-AVI-446 : Vulnérabilités dans Adobe Shockwave Player
- CERTA-2012-AVI-447 : Vulnérabilités dans HP Fortify
- CERTA-2012-AVI-448 : Vulnérabilités dans Adobe Reader X et Adobe Acrobat X
- CERTA-2012-AVI-449 : Vulnérabilité dans phpMyAdmin
- CERTA-2012-AVI-450 : Vulnérabilité dans HP Service Manager et HP Service Center Server
- CERTA-2012-AVI-451 : Vulnérabilité dans HP Service Manager Web Tier et HP Service Center Tier
- CERTA-2012-AVI-452 : Multiples vulnérabilités dans Java pour HP-UX
- CERTA-2012-AVI-453 : Vulnérabilité dans HP Integrity Server
- CERTA-2012-AVI-454 : Vulnérabilités dans Roundcube
- CERTA-2012-AVI-455 : Vulnérabilités dans PostgreSQL
- CERTA-2012-AVI-456 : Vulnérabilité dans Apple Remote Desktop
- CERTA-2012-AVI-457 : Multiples vulnérabilités dans Wireshark
- CERTA-2012-AVI-458 : Vulnérabilités dans Xen
- CERTA-2012-AVI-459 : Multiples vulnérabilités dans Adobe Flash Player
- CERTA-2012-AVI-460 : Multiples vulnérabilités dans Apache Web Server
- CERTA-2012-AVI-461 : Multiples vulnérabilités dans Lotus Domino
- CERTA-2012-AVI-462 : Vulnérabilité dans HP Serviceguard
- CERTA-2012-AVI-463 : Vulnérabilité dans certains produits Avaya
- CERTA-2012-AVI-464 : Vulnérabilité dans IBM Power Hardware Management Console

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

- CERTA-2012-ALE-003-003 : Vulnérabilité dans Microsoft XML Core Services (ajout de la solution)

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

24 août 2012 version initiale.