



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 02 décembre 2011
N° CERTA-2011-ACT-048

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2011-48

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-048>

Gestion du document

Référence	CERTA-2011-ACT-048
Titre	Bulletin d'actualité 2011-48
Date de la première version	02 décembre 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-048.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-048/>

1 Tunnel PPTP

Un incident récemment traité par le CERTA a mis en évidence le mode opératoire peu commun de l'attaquant. Celui-ci se connectait au réseau compromis par l'intermédiaire d'un tunnel PPTP (*Point-to-Point Tunneling Protocol*).

Le tunnel PPTP est une implémentation de VPN (*Virtual Private Network*). Il se décompose en deux parties :

- la gestion du canal de contrôle qui se fait par le port 1723/tcp ;
- l'échange des données, via un tunnel GRE (*Generic Routing Encapsulation*, protocole 47) qui encapsule des paquets PPP (*Point-to-Point Protocol*).

Les fonctionnalités de sécurité, telles que le chiffrement ou l'authentification, sont gérées au niveau de PPP.

Le CERTA recommande le filtrage, en entrée et en sortie, du port 1723/tcp, le tunnel ne pouvant s'établir lorsqu'il est privé de son canal de contrôle. Le filtrage du protocole GRE devrait aussi être mis en place.

Documentation :

- RFC 2637 - Point-to-Point Tunneling Protocol :
<http://tools.ietf.org/html/rfc2637>

2 Fichiers xdp

Le format de fichier `xdp` (*XML Data Package*) est un format créé par *Adobe* pour pouvoir assembler des fichiers `PDF` dans un fichier `XML`. Ce type de fichiers est ouvert par défaut par *Adobe Acrobat Reader* qui va lire les fichiers `PDF` contenus dedans, qui sont encodés en `base64`.

2.1 Problème de sécurité

Les fichiers `xdp` peuvent être utilisés par des attaquants pour embarquer un fichier `PDF` malveillant. En utilisant cette technique, ils peuvent contourner certains produits de sécurité.

Un tel exemple de fichier `xdp` malveillant a récemment été traité par le CERTA. Ce fichier est détecté comme malveillant par 3 anti-virus sur 42 sur *Virustotal*, alors que le fichier `PDF` contenu est détecté par 20 anti-virus sur 42. Ces chiffres montrent l'efficacité de cette encapsulation.

2.2 Recommandations

2.2.1 Mise à jour du logiciel

Une mise-à-jour régulière du lecteur *Adobe Acrobat Reader* constitue la meilleure des protections. Dans notre exemple, le fichier au format `XDP` encapsulait un document au format `PDF` exploitant une vulnérabilité connue et corrigée.

2.2.2 Analyse des messages reçus

Les fichiers `XDP` arrivant par courriels sont très rares. Il est recommandé de regarder si des pièces jointes avec cette extension sont arrivées pour analyser les messages concernés.

2.2.3 Modification de l'association XDP

Par défaut, lors de l'installation d'*Adobe Acrobat Reader*, les associations suivantes sont créées dans le registre (avec *Adobe X 10.1.1*) :

- `.acrobatsecuritysettings=AcroExch.acrobatsecuritysettings`
- `.api=AcroExch.Plugin`
- `.fdf=AcroExch.FDFDoc`
- `.pdf=AcroExch.Document`
- `.pdfxml=AcroExch.pdfxml`
- `.secstore=AcroExch.SecStore`
- `.xdp=AcroExch.XDPDoc`
- `.xdf=AcroExch.XFDFDoc`

Ces associations sont utilisées par *Windows* pour déterminer quelle application lancer lorsque l'on double-clique sur un fichier.

Afin de prévenir une exploitation malveillante de l'extension `.xdp`, il est possible de l'associer avec une autre application. Par exemple, on pourra associer l'extension avec *notepad* (type `txtfile`).

Pour désactiver l'association avec *Adobe Acrobat Reader*, exécuter la commande :

```
assoc .xdp=txtfile
reg.exe add HKCR\.xdp /v "Content Type" /d "text/xml" /f
```

Pour la réactiver:

```
assoc .xdp=AcroExch.XDPDoc
reg.exe add HKCR\.xdp /v "Content Type" /d "application/vnd.adobe.xdp+xml" /f
```

Cette désactivation permet de prévenir l'activation automatique de *Adobe Acrobat Reader* lors de l'ouverture d'un document `.xdp` (double-clic dans l'explorateur). Attention néanmoins, cette mesure ne prémunit pas d'une exploitation si l'utilisateur ouvre le fichier directement depuis l'application *Adobe Acrobat Reader* (Fichier -> Ouvrir). Enfin, nous attirons votre attention sur le risque de supprimer l'association (`assoc .xdp=`) qui déclenche une invite de l'utilisateur qui pourrait alors sélectionner *Adobe Acrobat Reader* et compromettre son poste.

Dans notre exemple avec `txtfile`, l'utilisateur verra s'ouvrir le bloc-notes de *Windows* avec le contenu du fichier `XML` (en cas d'ouverture via l'explorateur) ou un contenu en `XML` dans son navigateur.

Ces mesures ont été testées sur la plateforme suivante (configuration par défaut) :

Windows 7
Microsoft Office 2010 (Outlook)
Mozilla Firefox 8.0.1
Mozilla Thunderbird 6.0
Google Chrome 15.0.874.121

Nous vous recommandons de tester ces mesures dans votre environnement logiciel avant tout déploiement à grande échelle.

2.3 Références

- Description du format XDP :
http://partners.adobe.com/public/developer/en/xml/xdp_2.0.pdf
- Site de Virustotal :
<http://www.virustotal.com/>

3 Alerte du CERTA concernant une vulnérabilité dans FTPD

Cette semaine, le CERTA a émis une alerte concernant le service FTPD dans FreeBSD. En effet, une vulnérabilité permet à un utilisateur malintentionné de prendre le contrôle à distance du serveur avec des droits administrateur (*root*). Afin d'exploiter la vulnérabilité, l'attaquant doit avoir les droits nécessaires lui permettant de déposer des fichiers sur le serveur.

Des preuves de faisabilité sont présentes sur l'Internet. Un contournement provisoire est disponible afin d'empêcher ces fichiers d'être déposés (voir alerte CERTA-2011-ALE-007).

Documentation

- Alerte CERTA-2011-ALE-007 du 02 décembre 2011 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2011-ALE-007/>

4 Rappel des avis émis

Dans la période du 25 novembre au 02 décembre 2011, le CERTA a émis les publications suivantes :

- CERTA-2011-AVI-667 : Vulnérabilité dans IBM Tivoli Netcool/Reporter
- CERTA-2011-AVI-668 : Vulnérabilité dans Novell Open Enterprise Server
- CERTA-2011-AVI-669 : Vulnérabilité dans Lighttpd

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

Gestion détaillée du document

02 décembre 2011 version initiale.