Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 04 novembre 2011
N° CERTA-2011-ACT-044

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2011-44

Gestion du document

Référence	CERTA-2011-ACT-044
Titre	Bulletin d'actualité 2011-44
Date de la première version	04 novembre 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-044.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-044/

1 Alerte du CERTA sur l'exploitation d'une vulnérabilité non corrigée dans Microsoft Windows

Aujourd'hui le CERTA a alerté sur l'exploitation d'une vulnérabilité non corrigée dans Microsoft Windows.

Symantec et le *Laboratory of Cryptography and System Security (CrySys)* ont découvert une vulnérabilité non corrigée et exploitée sur l'Internet par le logiciel malveillant *Duqu*. Microsoft a publié un avis de sécurité 2639658 détaillant les mesures de protection immédiates pouvant être mises en œuvre.

Le logiciel malveillant Duqu se propage notamment via l'exploitation d'une vulnérabilité non corrigée dans les polices TrueType. À ce jour, le code malveillant utilise pour vecteur un document Microsoft Word mais toute application reposant sur la fonctionnalité des polices embarquées est potentiellement vulnérable. Pour mettre en œuvre exploitation de la vulnérabilité, l'attaquant va intégrer à un document une police malveillante dont le chargement par le système va déclencher l'exécution de code arbitraire. Au moment de la publication de cet avis, seuls des contournements provisoires sont disponibles. Une mise à jour de sécurité serait en cours de développement par Microsoft.

Documentation :

- Alerte CERTA :
  http://www.certa.ssi.gouv.fr/site/CERTA-2011-ALE-006/

2 Problème sérieux dans PHP

Une anomalie sérieuse a été détectée dans les versions 5.3.7 et 5.3.8 de PHP. Il est possible que d'autres versions de PHP soient concernées. Le problème émane du comportement de la fonction is_a(). Lorsque le premier paramètre passé à cette fonction n'est pas un objet, alors __autoload() est automatiquement appelé.

La définition de __autoload() est laissée à la discrétion des développeurs. Ainsi, dans un exemple pris du manuel de PHP5, la fonction est écrite de la façon suivante :

```
function __autoload ($class_name) {
include $class_name .  '.php';
}
```

Le manuel précise toutefois qu'il est recommandé de vérifier les données passées par les utilisateurs. Il faut cependant s'attendre à ce que cela ne soit pas fait systématiquement. Dans l'exemple mentionné, l'exécution de code arbitraire à distance est triviale si l'utilisateur peut manipuler $class_name. Il est donc vraisemblable que, avec ce comportement de la fonction is_a(), de nombreuses applications développées avec PHP soient vulnérables, avec pour effet l'exécution de code arbitraire à distance.

La fonction is_a() a fait l'objet d'une modification dans le SVN de PHP, qui peut être appliquée, en l'attente d'une nouvelle version de PHP5 (branche 3).

Documentation :

- Rapport de bogue 55475 de PHP :
  https://bugs.php.net/bug.php?id=55475
- Correction dans le SVN de PHP :
  http://svn.php.net/viewvc/?view=revision&revision=317183
- Manuel de PHP, rubrique *Autoloading Classes* :
  http://php.net/manual/en/language.oop5.autoload.php
- Référence CVE-2011-3379 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3379
  http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3379

3 Propagation d'un ver JBoss

3.1 Principe de fonctionnement

Un ver affecte actuellement les serveurs JBoss non mis à jour. Le ver se connecte aux jmx-console non protégées en utilisant une requête HTTP HEAD. L'utilisation de cette méthode permet d'outrepasser l'authentification de la console sur les versions vulnérables et d'installer un *package* permettant d'executer des commandes arbitraires.

La requête effectuée par le ver se présente sous la forme suivante :

```
HEAD /jmx-console/HtmlAdaptor?action=invokeOpByName&name=jboss.admin%3Aservice%3D
DeploymentFileRepository&methodName=store&argType=java.lang.String&arg0=
iddqd.war&argType=java.lang.String&arg1=iddqd&argType=java.lang.String&arg2=
.jsp&argType=java.lang.String&arg3=...
```

Des commandes sont ensuite automatiquement envoyées au serveur afin de lancer le télechargement de code permettant la propagation du ver.

3.2 Vulnérabilité exploitée

La vulnérabilité exploitée n'est pas nouvelle (CVE-2010-0738) et se situe dans la configuration de la jmx-console définie dans le fichier deploy/jmx-console.war/WEB-INF/web.xml. Par défaut, les

contraintes de sécurité définies ne requièrent d'authentification que pour les methodes GET et POST, laissant les autres requêtes HTTP accèder librement à la console.

Il est donc recommandé de vérifier la bonne configuration de la `jmx-console` et d'appliquer les mises à jour nécessaires le cas échéant.

Exemple de fichier de web.xml vulnérable :

```
<security-constraint>
  <web-resource-collection>
    <web-resource-name>HtmlAdaptor</web-resource-name>
    <description>
       An example security config that only allows users with the role
       JBossAdmin to access the HTML JMX console web application
    </description>
    <url-pattern>/*</url-pattern>
    <http-method>GET</http-method>
    <http-method>POST</http-method>
  </web-resource-collection>
  <auth-constraint>
    <role-name>JBossAdmin</role-name>
  </auth-constraint>
</security-constraint>
```

Le retrait des lignes `http-method` corrige le problème en appliquant les contraintes sur l'ensemble des methodes HTTP. Les versions 6.x et 7.x de JBoss corrigent cette vulnérabilité.

Documentation :

- Site Officiel JBoss :
  http://www.jboss.org
- Référence CVE CVE-2010-0738 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0738
- Sécurisation de la jmx-console :
  http://community.jboss.org/wiki/SecureTheJmxConsole

4 Rappel des avis émis

Dans la période du 28 octobre au 03 novembre 2011, le CERTA a émis les publications suivantes :

- CERTA-2011-AVI-597 : Vulnérabilités dans Apple QuickTime
- CERTA-2011-AVI-598 : Vulnérabilité dans Novell iPrint
- CERTA-2011-AVI-599 : Vulnérabilité dans OpenLDAP
- CERTA-2011-AVI-600 : Vulnérabilité dans Zope
- CERTA-2011-AVI-601 : Vulnérabilité dans Cisco CUCM, UCCX et Unified IP-IVR
- CERTA-2011-AVI-602 : Vulnérabilité dans des caméras Cisco
- CERTA-2011-AVI-603 : Vulnérabilités dans Cisco Security Agent
- CERTA-2011-AVI-604 : Vulnérabilité dans Novell ZENworks
- CERTA-2011-AVI-605 : Vulnérabilités dans des produits CheckPoint
- CERTA-2011-AVI-606 : Vulnérabilités dans Cisco Webex Player
- CERTA-2011-AVI-607 : Vulnérabilités dans Fujitsu Interstage HTTP Server
- CERTA-2011-AVI-608 : Vulnérabilité dans les produits D-Link
- CERTA-2011-AVI-609 : Multiples vulnérabilités dans les produits VMWare
- CERTA-2011-AVI-610 : Vulnérabilité dans IBM Lotus Sametime
- CERTA-2011-AVI-611 : Multiples vulnérabilités dans HP OpenView
- CERTA-2011-AVI-612 : Multiples vulnérabilités dans Wireshark
- CERTA-2011-AVI-613 : Vulnérabilité dans les produits Cisco Small Business SRP500 Series
- CERTA-2011-AVI-614 : Vulnérabilité dans Novell Messenger
- CERTA-2011-AVI-615 : Vulnérabilité dans Squid
- CERTA-2011-AVI-616 : Vulnérabilités dans IBM AIX Bind

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 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.

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 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.

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

04 novembre 2011 version initiale.