



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 17 février 2012
N° CERTA-2012-ACT-007

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2012-07

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-2012-ACT-007>

Gestion du document

Référence	CERTA-2012-ACT-007
Titre	Bulletin d'actualité 2012-07
Date de la première version	17 février 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 Piégeage d'un dépôt FTP de logiciel

Le projet Horde produit plusieurs logiciels libres de travail collaboratif, dont IMP, un serveur de messagerie POP et IMAP.

Incident révélé

En novembre 2011, suite à une intrusion sur un serveur FTP du projet, trois paquets logiciels ont été piégés. Une porte dérobée a été incluse dans ces paquets, permettant à un attaquant d'exécuter du code à distance.

Les logiciels concernés sont :

- Horde 3.3.12, téléchargé entre le 15 novembre 2011 et le 07 février 2012 ;
- Horde Groupware 1.2.10, téléchargé entre le 09 novembre 2011 et le 07 février 2012 ;
- Horde Groupware Webmail Edition 1.2.10, téléchargé entre le 02 novembre 2011 et le 07 février 2012.

Si vous avez le moindre doute sur votre version, le projet indique une chaîne de caractères révélatrice des versions piégées, à chercher dans le répertoire d'installation : `$m[1] ($m[2])`

Selon l'équipe du projet, seul le serveur FTP `ftp.horde.org` est concerné. Le serveur a été remplacé et les analyses se poursuivent.

Dans la communication sur l'incident, les développeurs du projet ont suggéré des versions de remplacement accompagnées de leurs condensés MD5.

Recommandations

Le CERTA recommande, pour ce cas précis :

- de vérifier les versions téléchargées (dates, caractéristiques...);
- au moindre doute, et surtout en cas de découverte de versions malveillantes, de remplacer le paquet utilisé;
- de comparer le condensé MD5 du paquet téléchargé au condensé indiqué dans l'annonce sur l'incident.

De manière plus générale, la plus grande attention doit être portée sur les téléchargements de logiciels ou de correctifs :

- le site de l'éditeur ou un miroir officiel doit être privilégié ;
- l'intégrité du contenu téléchargé doit être vérifiée, dès lors que cette vérification est possible ;
- les communications (site Web, listes de diffusion...) de l'éditeur ou du projet doivent être surveillées pour être informé au plus tôt d'incidents, comme celui que le projet Horde vient de subir ;
- pour un correctif, une étude sur le code source ou sur les modifications peut également être envisagée ;
- l'exécution et l'observation sur une plateforme de test peuvent révéler des anomalies.

Documentation

- Note d'information du CERTA CERTA-2001-INF-004 « Acquisition des correctifs » :
<http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-004/index.html>
- Annonce du projet Horde du 13 février 2012 :
<http://lists.horde.org/archives/annonce/2012/000751.html>
- Référence CVE CVE-2012-0209 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0209>

2 Mise à jour mensuelle Microsoft

Cette semaine, Microsoft a publié plusieurs correctifs de sécurité. Sur les neuf bulletins édités, quatre sont jugés critiques par Microsoft et les cinq autres sont considérés comme importants.

Les vulnérabilités corrigées permettaient :

- une exécution de code arbitraire à distance ;
- une élévation de privilèges ;
- une divulgation d'information ;
- une injection de code indirecte à distance.

Les produits Microsoft impactés par ces mises à jour sont:

- Microsoft Windows (toutes versions) ;
- Internet Explorer (toutes versions) ;
- Microsoft .Net Framework 2.0, 3.5.1 et 4.0 ;
- Microsoft Silverlight 4 ;
- Microsoft Sharepoint 2010 ;
- Microsoft Visio Viewer 2010.

Le CERTA recommande l'application de ces mises à jour dès que possible.

Documentation

- Synthèse des bulletins de sécurité Microsoft du mois de janvier 2012:
<http://technet.microsoft.com/fr-fr/security/bulletin/ms12-feb>
- CERTA-2012-AVI-082 Vulnérabilités dans le Framework Microsoft .Net et Microsoft Silverlight
<http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-082/index.html>
- CERTA-2012-AVI-081 Multiples vulnérabilités dans Microsoft Visio Viewer
<http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-081/index.html>
- CERTA-2012-AVI-080 Vulnérabilité dans le codec Indeo de Microsoft Windows
<http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-080/index.html>

- CERTA-2012-AVI-079 Vulnérabilité dans la bibliothèque RunTime C Microsoft
<http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-079/index.html>
- CERTA-2012-AVI-078 Vulnérabilité dans le panneau de configuration des couleurs de Microsoft Windows
<http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-078/index.html>
- CERTA-2012-AVI-077 Vulnérabilités dans Microsoft Sharepoint
<http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-077/index.html>
- CERTA-2012-AVI-076 Multiples vulnérabilités dans Internet Explorer
<http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-076/index.html>
- CERTA-2012-AVI-075 Vulnérabilités dans le pilote de gestion des connexions réseau de Microsoft Windows
<http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-075/index.html>
- CERTA-2012-AVI-074 Vulnérabilités dans les pilotes Windows
<http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-074/index.html>

3 Rappel des avis émis

Dans la période du 10 février 2012 au 16 février 2012, le CERTA a émis les publications suivantes :

- CERTA-2012-AVI-071 : Vulnérabilités dans Novell iPrint
- CERTA-2012-AVI-072 : Vulnérabilités dans des produits Horde
- CERTA-2012-AVI-073 : Vulnérabilité dans les produits Mozilla
- CERTA-2012-AVI-074 : Vulnérabilités dans les pilotes Windows
- CERTA-2012-AVI-075 : Vulnérabilités dans le pilote de gestion des connexions réseau de Microsoft Windows
- CERTA-2012-AVI-076 : Multiples vulnérabilités dans Internet Explorer
- CERTA-2012-AVI-077 : Vulnérabilités dans Microsoft Sharepoint
- CERTA-2012-AVI-078 : Vulnérabilité dans le panneau de configuration des couleurs de Microsoft Windows
- CERTA-2012-AVI-079 : Vulnérabilité dans la bibliothèque RunTime C Microsoft
- CERTA-2012-AVI-080 : Vulnérabilité dans le codec Indeo de Microsoft Windows
- CERTA-2012-AVI-081 : Multiples vulnérabilités dans Microsoft Visio Viewer
- CERTA-2012-AVI-082 : Vulnérabilités dans le Framework Microsoft Net et Microsoft Silverlight

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 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.

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 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.

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

17 février 2012 version initiale.