Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 06 septembre 2013
N° CERTA-2013-ACT-036

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2013-ACT-036

1 Fin de support de Microsoft Windows XP

Microsoft a planifié l'arrêt du support de Microsoft Windows XP en **avril 2014**. À cette date, l'éditeur cessera d'assurer la publication de correctifs de sécurité, y compris en cas de découverte d'une vulnérabilité critique.

En ce qui concerne le système d'exploitation Windows XP, un grand nombre de mécanismes de sécurité sont absents, à l'inverse de Windows 8 ou Windows 7. L'absence de tels mécanismes facilite la prise de contrôle par un attaquant à l'aide de techniques d'exploitation largement diffusées.

Il est important de souligner que l'arrêt du support de Windows XP va entraîner une recrudescence des codes d'exploitations de type « 0-day » dans les kits d'exploitation. Les vendeurs de vulnérabilités vont probablement profiter d'écouler leur réserve de « 0-day » qui auront d'autant plus de valeur pour les attaquants car les vulnérabilités ne seront pas corrigées par l'éditeur.

Le support et la mise à disposition de mises à jour de sécurité par l'éditeur sont un point crucial à la sécurisation d'un serveur ou d'une station de travail. L'arrêt du support d'une version de système d'exploitation doit être anticipé et constitue une motivation à la migration vers une version récente. Cela concerne en majorité les postes de travail mais peut également concerner des équipements intégrés embarquant le système Windows XP (ex : équipements industriels, médicaux, interfaces utilisateur, etc...). Pour ces derniers, pouvant faire l'objet de contraintes métier, une démarche spécifique doit être engagée, en coordination avec le fournisseur, afin d'étudier les différents scenarios envisageables.

De plus, la durée de vie du système d'exploitation retenu pour la migration doit être adaptée au cycle de vie des projets et à la vitesse de renouvellement du parc informatique. Une période de cinq ans minimum est recommandée pour les environnements bureautiques.

De nombreux systèmes utilisant Microsoft Windows XP sont aujourd'hui encore en service dans les administrations et les entreprises. Le CERTA attire l'attention sur la nécessité d'anticiper dès à présent une migration vers des systèmes dont la pérennité des mises à jour de sécurité pourra être assurée après cette date.

2 Synchronisation horaire dans le cadre du traitement d'incident

Dans le cadre de sa mission de traitement des attaques informatiques, le CERTA est encore régulièrement confronté à des analyses de systèmes pour lesquels la synchronisation horaire n'est pas assurée.

Lors du traitement d'un incident, les journaux d'évènements et traces systèmes constituent une source essentielle à la fois dans la détection *a priori* d'un incident de sécurité mais également lors de l'analyse d'une compromission *a posteriori* pour comprendre précisément le déroulement de l'attaque.

Une chronologie des actions de l'attaquant est généralement établie afin de déterminer son cheminement au sein du SI, les faiblesses potentiellement exploitées ainsi que les conséquences de l'incident pour la victime (exfiltration de données, atteinte à la continuité de service ou à la confidentialité de données, etc).

Cette chronologie est établie via la corrélation d'évènements des différents journaux (routeurs, serveurs mandataires, serveurs de messagerie, contrôleurs de domaine, etc.) et traces sur les systèmes (opérations sur les fichiers), il est donc nécessaire d'avoir une base de temps commune et fiable entre ces différents systèmes.

Le CERTA recommande fortement l'utilisation d'un serveur de temps utilisant le protocole NTP, en particulier dans sa version 4 qui permet l'authentification par certificats, afin de synchroniser les serveurs, les équipements réseaux et les postes de travail, tout en prenant garde à définir par avance un fuseau horaire commun qui ne sera pas perturbé par l'heure d'été (UTC) ou la position géographique sur Terre.

Documentation

– Note d'information CERTA-2008-INF-005 sur la gestion des journaux d'évènements (articles 3.2 et 3.3)
http://www.certa.ssi.gouv.fr/site/CERTA-2008-INF-005/

3 Réaction aux dénis de service distribués

Le CERTA est régulièrement sollicité pour des attaques par saturation sur des serveurs Internet dites «déni de service distribué».

Dans ces situations, l'acteur le plus à même de réagir est le fournisseur d'accès Internet, qui proposent souvent des dispositifs de contre-mesure efficaces.

La gestion de ce type d'incident est largement facilitée si l'administrateur du site les a anticipé en prenant contact avec son FAI, afin de se renseigner sur les différentes solutions envisageables et pour préparer un plan de réaction.

Le CERTA recommande aux administrateurs de sites potentiellement concernés par ce type de menaces de se mettre en rapport avec leur fournisseur d'accès dès à présent, afin d'identifier les points de contact à solliciter en cas d'urgence, de sorte à ne pas être pris au dépourvu face à une attaque.

Pour mémoire, la note d'information CERTA-2012-INF-001 propose des mesures visant à anticiper et gérer les attaques en déni de service.

Documentation

– Note d'information CERTA-2012-INF-001 sur la prévention et la réaction aux dénis de service :
http://www.certa.ssi.gouv.fr/site/CERTA-2012-INF-001/

4 Rappel des avis émis

Dans la période du 30 août au 05 septembre 2013, le CERTA a émis les publications suivantes :

– CERTA-2013-AVI-498 : Multiples vulnérabilités dans le noyau Linux de Debian
– CERTA-2013-AVI-499 : Vulnérabilité dans VMware ESXi et ESX
– CERTA-2013-AVI-500 : Multiples vulnérabilités dans Asterisk
– CERTA-2013-AVI-501 : Multiples vulnérabilités dans Citrix CloudPortal Services Manager
– CERTA-2013-AVI-502 : Multiples vulnérabilités dans MediaWiki
– CERTA-2013-AVI-503 : Multiples vulnérabilités dans Cisco WebEx
– CERTA-2013-AVI-504 : Vulnérabilité dans le système SCADA Schneider Electric OFS

Gestion détaillée du document

06 septembre 2013 version initiale.