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 mai 2013
N° CERTA-2013-ACT-020

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2013-ACT-020

1 - Recommandation pour la sécurisation des sites Web

L'ANSSI a publié le 13 mai 2013 une note technique proposant des recommandations sur la sécurisation d'environnements Web.

De par leur exposition sur l'Internet, les serveurs Web et les applications qu'ils hébergent sont des cibles de choix pour des attaques informatiques. Cette note présente, aux administrateurs et aux développeurs, des recommandations techniques à mettre en place pour limiter le risque de compromission de plates-formes Web, ainsi que les bonnes pratiques de détection d'incidents et de réaction sur incident.

Le CERTA recommande la lecture de cette note technique et l'application des recommandations qu'elle contient.

Documentation

– Recommandations pour la sécurisation des sites Web :
http://www.ssi.gouv.fr/IMG/pdf/NP_Securite_Web_NoteTech.pdf

2 - Vulnérabilité dans le noyau Linux

Le 13 avril 2013 une vulnérabilité a été corrigée dans le noyau Linux. Elle permet à un utilisateur non privilégié mais autorisé à exécuter du code, d'obtenir l'ensemble des droits sur un serveur vulnérable.

Cette vulnérabilité de type « élévation de privilège » trouve sa source dans une erreur de programmation du code noyau : l'insuffisance de validation d'un paramètre de l'appel système « sys_perf_event_open » mène à une possibilité d'exécution de code arbitraire en mode noyau, pouvant être utilisée afin d'élever les privilèges de l'utilisateur, qui peut alors prendre le contrôle total du système.

Les correctifs de sécurité ne sont actuellement pas encore disponibles en version stable pour la plupart des distributions Linux. De plus, étant donnée la diffusion d'un code fonctionnel exploitant cette vulnérabilité, le CERTA recommande de veiller à l'installation du correctif de sécurité dès sa mise à disposition, ainsi qu'à l'application, dans la mesure du possible, des mesures de contournement provisoires indiquées dans l'alerte CERTA du 14 mai 2013.

Il est également recommandé de faire preuve d'une surveillance accrue des systèmes vulnérables (analyse des journaux et du système de fichiers), afin de détecter rapidement toutes activités anormales pouvant être un signe de compromission, comme l'ajout d'un utilisateur, le lancement d'un service ou la création de fichiers suspects.

Documentation

– Alerte CERTA-2013-ALE-005 du 14 mai 2013 :
http://www.certa.ssi.gouv.fr/site/CERTA-2013-ALE-005/

3 - Mise à jour mensuelle Microsoft

Lors de la mise à jour mensuelle de Microsoft, dix bulletins de sécurité ont été publiés.

Deux bulletins sont considérés comme critiques :

- MS13-037 qui concerne Microsoft Internet Explorer, cette mise à jour corrige dix vulnérabilités permettant à un attaquant, à l'aide d'une page Web spécialement conçue, d'exécuter du code arbitraire à distance ;
- MS13-038 qui concerne Internet Explorer 8, cette mise à jour corrige la vulnérabilité évoquée dans l'alerte CERTA-2013-ALE-003. Cette mise à jour ferme donc l'alerte de sécurité.

Huit bulletins sont considérés comme importants, ils concernent :

- une vulnérabilité dans Microsoft Windows HTTP.sys (MS13-039) ;
- des vulnérabilités dans Microsoft .NET Framework (MS13-040) ;
- une vulnérabilité dans Microsoft Lync (MS13-041) ;
- des vulnérabilités dans Microsoft Publisher (MS13-042) ;
- une vulnérabilité dans Microsoft Word (MS13-043) ;
- une vulnérabilité dans Microsoft Visio (MS13-044) ;
- une vulnérabilité dans Microsoft Windows Essentials (MS13-045) ;
- des vulnérabilités dans le noyau Microsoft Windows (MS13-046).

Le CERTA recommande l'application de ces correctifs dès que possible.

Documentation

- Synthèse des bulletins de sécurité Microsoft du mois de mai 2013 :
  http://technet.microsoft.com/fr-fr/security/bulletin/ms13-may
- Alerte CERTA-2013-ALE-003 du 06 mai 2013 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-ALE-003/

4 - Mise à jour Adobe

Le 14 mai 2013, Adobe a publié trois bulletins concernant des correctifs de sécurité :

- APSB13-15 qui concerne Adobe Reader ;
- APSB13-14 qui concerne Adobe Flash Player ;
- APSB13-13 qui concerne Adobe ColdFusion.

Cette dernière mise à jour corrige la vulnérabilité évoquée dans l'alerte CERTA-2013-ALE-004, et ferme donc celle-ci.

Le CERTA recommande l'application de ces correctifs dès que possible.

Documentation

- Synthèse des bulletins de sécurité publiés par Adobe :
  http://www.adobe.com/support/security
- Alerte CERTA-2013-ALE-004 du 10 mai 2013 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-ALE-004/

5 - Rappel des avis émis

Dans la période du 10 au 16 mai 2013, le CERTA a émis les publications suivantes :

- CERTA-2013-ALE-005 : Vulnérabilité dans le noyau Linux
- CERTA-2013-AVI-295 : Multiples vulnérabilités dans EMC Documentum
- CERTA-2013-AVI-296 : Vulnérabilité dans EMC AlphaStor
- CERTA-2013-AVI-297 : Multiples vulnérabilités dans Cisco Unified Customer Voice Portal
- CERTA-2013-AVI-298 : Vulnérabilité dans EMC RSA Authentication Agent

– CERTA-2013-AVI-299 : Vulnérabilité dans Microsoft Internet Explorer
– CERTA-2013-AVI-300 : Vulnérabilité dans Microsoft Internet Explorer 8
– CERTA-2013-AVI-301 : Vulnérabilité dans Microsoft Windows HTTPsys
– CERTA-2013-AVI-302 : Multiples vulnérabilités dans Microsoft NET Framework
– CERTA-2013-AVI-303 : Vulnérabilité dans Microsoft Lync
– CERTA-2013-AVI-304 : Multiples vulnérabilités dans Microsoft Publisher
– CERTA-2013-AVI-305 : Vulnérabilité dans Microsoft Word
– CERTA-2013-AVI-306 : Vulnérabilité dans Microsoft Visio
– CERTA-2013-AVI-307 : Vulnérabilité dans Microsoft Windows Essentials
– CERTA-2013-AVI-308 : Multiples vulnérabilités dans le noyau Microsoft Windows
– CERTA-2013-AVI-309 : Multiples vulnérabilités dans les produits Mozilla
– CERTA-2013-AVI-310 : Multiples vulnérabilités dans Adobe Reader
– CERTA-2013-AVI-311 : Multiples vulnérabilités dans Adobe Flash Player
– CERTA-2013-AVI-312 : Multiples vulnérabilités dans Adobe ColdFusion
– CERTA-2013-AVI-313 : Vulnérabilité dans Cisco TelePresence Supervisor MSE 8050
– CERTA-2013-AVI-314 : Vulnérabilité dans Huawei Quidway

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

– CERTA-2013-ALE-003-002 : Vulnérabilité dans Microsoft Internet Explorer 8 (fermeture de l'alerte, suite à la diffusion du correctif par l'éditeur)
– CERTA-2013-ALE-004-001 : Vulnérabilité dans Adobe ColdFusion (fermeture de l'alerte, suite à la diffusion du correctif par l'éditeur)

Gestion détaillée du document

17 mai 2013 version initiale.