Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 15 février 2013
N° CERTA-2013-ACT-007

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2013-ACT-007

1 Mise à jour mensuelle Microsoft

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

Cinq bulletins sont considérés comme critiques :

- MS13-009 qui concerne Microsoft Internet Explorer, cette mise à jour corrige treize vulnérabilités permettant à un attaquant, à l'aide d'une page Web spécialement conçue, d'exécuter du code arbitraire à distance ;
- MS13-010 qui concerne Microsoft Vector Markup Language, cette mise à jour corrige une vulnérabilité permettant à un attaquant, à l'aide d'une page Web spécialement conçue, d'exécuter du code arbitraire à distance.
- MS13-011 qui concerne Microsoft DirectShow Media Decompression, cette mise à jour corrige une vulnérabilité permettant à un attaquant, à l'aide d'un fichier multimedia spécialement conçu, d'exécuter du code arbitraire à distance.
- MS13-012 qui concerne Microsoft Exchange Server, cette mise à jour corrige des vulnérabilités permettant à un attaquant, à l'aide d'un fichier spécialement conçu, d'exécuter du code arbitraire à distance.
- MS13-020 qui concerne Microsoft OLE Automation, cette mise à jour corrige une vulnérabilité permettant à un attaquant, à l'aide d'un fichier spécialement conçu, d'exécuter du code arbitraire à distance.

Sept bulletins sont considérés comme importants, ils concernent :

- des vulnérabilités dans Microsoft Fast Search Server 2010 (MS13-013) ;
- une vulnérabilité dans Microsoft NFS (MS13-014) ;
- une vulnérabilité dans Microsoft .NET Framework (MS13-015) ;
- des vulnérabilités dans les pilotes en mode noyau de Microsoft Windows (MS13-016) ;
- des vulnérabilités dans le noyau de Microsoft Windows (MS13-017) ;
- une vulnérabilité dans Microsoft TCP/IP (MS13-018) ;
- une vulnérabilité dans Microsoft CSRSS (MS13-019).

Microsoft a constaté que le CVE-2013-0030 (MS13-010) a été utilisé dans des attaques ciblées, et que les CVE-2013-0077 (MS13-011), MS13-012, MS13-013 et CVE-2013-0076 (MS13-019) ont été révélés publiquement. Le code d'exploitation pour le CVE-2013-0025 (MS13-009) est disponible publiquement et est activement utilisé.

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

Documentation

- Synthèse des bulletins de sécurité Microsoft du mois de février 2013 :
  http://technet.microsoft.com/security/bulletin/ms13-feb

- Avis CERTA-2013-AVI-113 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-113/
- Avis CERTA-2013-AVI-114 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-114/
- Avis CERTA-2013-AVI-115 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-115/
- Avis CERTA-2013-AVI-116 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-116/
- Avis CERTA-2013-AVI-117 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-117/
- Avis CERTA-2013-AVI-118 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-118/
- Avis CERTA-2013-AVI-119 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-119/
- Avis CERTA-2013-AVI-120 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-120/
- Avis CERTA-2013-AVI-121 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-121/
- Avis CERTA-2013-AVI-122 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-122/
- Avis CERTA-2013-AVI-123 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-123/
- Avis CERTA-2013-AVI-124 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-124/

2 Alerte dans Adobe Reader et Acrobat

Cette semaine le CERTA a diffusé l'alerte CERTA-2013-ALE-002, concernant deux vulnérabilités majeures dans Adobe Reader et Acrobat. Les failles permettent d'exécuter du code arbitraire à distance au moyen d'un fichier PDF spécialement conçu. Elles ont été largement diffusées et sont activement exploitées. Dans le cas où Adobe Reader ou Acrobat ne sont pas nécessaires, il est recommandé de désactiver ces logiciels le temps qu'un correctif soit disponible. L'éditeur prévoie la diffusion d'un correctif de sécurité.

En revanche, si Adobe Reader ou Acrobat sont requis, la solution proposée par l'éditeur est d'utiliser le mode « Protected View » d'Adobe, qui permet de cloisonner (sandbox) le lecteur PDF. En plus de la solution de l'éditeur, le CERTA préconise de désactiver JavaScript dans le lecteur PDF et d'utiliser la version « XI » d'Adobe Reader ou Acrobat.

Nous recommandons également de ne pas ouvrir de documents PDF qui ne sont pas de confiance :

- issu d'un site Web inconnu ;
- en pièce jointe d'un courriel douteux (expéditeur inconnu, contenu incohérent, etc.).

Le CERTA rappelle qu'Adobe a corrigé cette semaine de multiples vulnérabilités dans Adobe Flash Player et Adobe Shockwave Player (CERTA-2013-AVI-127, CERTA-2013-AVI-125 et CERTA-2013-AVI-104).

Documentation

- Alerte Adobe Reader et Acrobat CERTA-2013-ALE-002 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-ALE-002/
- Avis CERTA-2013-AVI-127 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-127/
- Avis CERTA-2013-AVI-125 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-125/
- Avis CERTA-2013-AVI-104 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-104/

3 Compromission de la société Bit9 et protection des éléments secrets

La société Bit9 propose une solution permettant de vérifier si un programme est inscrit dans une liste blanche. Contrairement aux antivirus qui identifient les fichiers infectés en utilisant des listes noires, ce système permet de déterminer les fichiers connus comme étant sains. Cette solution permet également de vérifier la signature numérique des logiciels. En particulier, tout programme signé par la société est considéré comme sain. Le 8 février 2013, Bit9 a annoncé avoir subi une intrusion dans ses systèmes d'information. D'après les investigations menées, seul leur programme permettant de signer numériquement des applications a été touché. Trois de leurs clients auraient ainsi été victimes de codes malveillants signés par un certificat valide et appartenant à Bit9.

Cet incident illustre bien la nécessité de protéger aussi bien les clefs privées que le mécanisme mis en place pour réaliser les opérations cryptographiques (signature ou chiffrement). Comme le recommande l'annexe B2 du RGS, « de par leur nature même, les éléments privés ou secrets ne peuvent être employés que dans un environnement de confiance ». La confiance de l'environnement peut être, par exemple, renforcée par l'utilisation de *hardware security modules* (HSM), dont certains ont été certifiés par l'ANSSI. Le CERTA souligne également l'importance de vérifier les révocations de certificat.

Documentation

- Annonce officielle de Bit9 :
  https://blog.bit9.com/2013/02/08/bit9-and-our-customers-security/
- Annexe B2 du Référentiel général de sécurité :
  http://www.ssi.gouv.fr/IMG/pdf/RGS_B_2.pdf
- Liste des produits HSM certifiés :
  http://www.ssi.gouv.fr/fr/produits-et-prestataires/sscd-hsm-certifies/tableau-des-produits-certifies-conformes-psc.html

4 Rappel des avis émis

Dans la période du 8 février au 15 février 2013, le CERTA a émis les publications suivantes :

- CERTA-2013-ALE-002 : Vulnérabilités dans Adobe Reader et Acrobat
- CERTA-2013-AVI-103 : Vulnérabilité dans PostgreSQL
- CERTA-2013-AVI-104 : Multiples vulnérabilités dans Adobe Flash Player
- CERTA-2013-AVI-105 : Vulnérabilité dans VMware
- CERTA-2013-AVI-106 : Multiples vulnérabilités dans HP LeftHand Virtual SAN Appliance hydra
- CERTA-2013-AVI-107 : Vulnérabilité dans cURL libcurl
- CERTA-2013-AVI-108 : Multiples vulnérabilités dans IBM Netezza WebAdmin
- CERTA-2013-AVI-109 : Vulnérabilité dans GnuTLS
- CERTA-2013-AVI-110 : Multiples vulnérabilités dans Microsoft Windows Flash Player
- CERTA-2013-AVI-111 : Multiples vulnérabilités dans IBM InfoSphere
- CERTA-2013-AVI-112 : Multiples vulnérabilités dans IBM Tivoli
- CERTA-2013-AVI-113 : Multiples vulnérabilités dans Microsoft Internet Explorer
- CERTA-2013-AVI-114 : Vulnérabilité dans Microsoft Vector Markup Language
- CERTA-2013-AVI-115 : Vulnérabilité dans Microsoft DirectShow Media Decompression
- CERTA-2013-AVI-116 : Multiples vulnérabilités dans Microsoft Exchange Server
- CERTA-2013-AVI-117 : Vulnérabilité dans Microsoft FAST Search Server 2010
- CERTA-2013-AVI-118 : Vulnérabilité dans Microsoft NFS Server
- CERTA-2013-AVI-119 : Vulnérabilité dans Microsoft NET Framework
- CERTA-2013-AVI-120 : Multiples vulnérabilités dans Microsoft Windows Kernel-Mode Driver
- CERTA-2013-AVI-121 : Multiples vulnérabilités dans Microsoft Windows Kernel
- CERTA-2013-AVI-122 : Vulnérabilité dans Microsoft Windows TCP/IP
- CERTA-2013-AVI-123 : Vulnérabilité dans Microsoft CSRSS
- CERTA-2013-AVI-124 : Vulnérabilité dans Microsoft OLE Automation

- CERTA-2013-AVI-125 : Multiples vulnérabilités dans Adobe Shockwave Player
- CERTA-2013-AVI-126 : Multiples vulnérabilités dans Google Chrome Adobe Flash Player
- CERTA-2013-AVI-127 : Multiples vulnérabilités dans Adobe Flash Player
- CERTA-2013-AVI-128 : Vulnérabilité dans Cisco Unified MeetingPlace
- CERTA-2013-AVI-129 : Vulnérabilité dans le système SCADA Moxa EDR-G903
- CERTA-2013-AVI-130 : Vulnérabilité dans IBM WebSphere

Gestion détaillée du document

15 février 2013 version initiale.