Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 28 décembre 2012
N° CERTA-2012-ACT-052

**Affaire suivie par :**
CERTA

# BULLETIN D'ACTUALITÉ

**Objet : Bulletin d'actualité CERTA-2012-ACT-052**

| | |
|---|---|
| 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-052` |

## 1 Vulnérabilité dans les pilotes Nvidia

Cette semaine le CERTA a publié une alerte concernant une vulnérabilité dans le service *NVidia Driver Helper Service*. Ce service est installé par les pilotes de certaines cartes graphiques *NVidia*. La vulnérabilité se situe au niveau du canal nommé utilisé pour communiquer avec le service. Ce canal peut également être utilisé depuis un poste distant, sous réserve de disposer des droits d'accès. C'est généralement le cas quand le poste est intégré à un domaine et que des utilisateurs de ce domaine peuvent y accéder.

Un outil exploitant automatiquement cette vulnérabilité est largement diffusé sur l'Internet. S'il possède un compte légitime sur une machine équipée d'une carte graphique *NVidia*, un attaquant peut ainsi facilement exécuter du code arbitraire à distance avec les droits système sur cette machine. Ce scénario est plausible avec les comptes d'un domaine. Dans le cas où le canal n'est pas accessible depuis le réseau, le risque d'élévation de privilèges en local reste présent.

### Documentation

- Alerte CERTA-2012-ALE-009 du 26 décembre 2012 :
  `http://www.certa.ssi.gouv.fr/site/CERTA-2012-ALE-009/`

## 2 Nouvelle clé PGP pour le CERTA

À compter du 1er janvier 2013, la clé PGP du CERTA change. Celle-ci peut être utilisée pour communiquer des éléments sensibles, mais non classifiés.

Afin de garantir sa légitimité, cette nouvelle clé a été signée par l'ancienne, qui restera disponible sur le site du CERTA pour référence.

L'empreinte de la nouvelle clé, d'identifiant 0x1B45CF2A, est :
7F4C 8FA6 A356 D1CC 2E5C AB09 5416 33B8 1B45 CF2A

### Documentation

- Nouvelle clé PGP :
  `http://www.certa.ssi.gouv.fr/certa/public_key.asc`
- Page « Nous contacter » :
  `http://www.certa.ssi.gouv.fr/certa/contact.html`

# 3 En 2013, le CERTA et l'ANSSI recrutent

Vous souhaitez participer activement à l'effort de défense de votre pays ?

Vous êtes passionné et disposez de réelles compétences dans le domaine de la sécurité des systèmes d'information ?

Vous recherchez l'engagement opérationnel et l'excellence technique ?

Rejoignez-nous !

Dans le cadre de la poursuite de la montée en puissance de l'ANSSI, le CERTA recherche en 2013 :

- des ingénieurs en investigation numérique :
  `http://www.ssi.gouv.fr/IMG/pdf/FdP_ANSSI_COSSI_DTO_FRI_Ingenieur_en_investigation_numerique-v2-0.pdf`
- des assistants en traitement d'incident informatique :
  `http://www.ssi.gouv.fr/IMG/pdf/FdP_ANSSI_COSSI_DTO_FRI_Assistant_en_traitement_incident_informatique_v2-0.pdf`
- des ingénieurs chargés d'analyse en détection d'intrusions :
  `http://www.ssi.gouv.fr/IMG/pdf/FdP_ANSSI_COSSI_DTO_FRI_Analyste_en_detection_d_intrusion.pdf`

De nombreux autres postes sont également proposés par l'ANSSI :
`http://www.ssi.gouv.fr/fr/anssi/emploi/`

Les candidatures sont à adresser par courrier électronique à : recrutement@ssi.gouv.fr

# 4 Bilan de l'année 2012

Comme il est de coutume, cette fin d'année est l'occasion de faire quelques bilans.

Comme les années précédentes, 2012 aura été une année dense en activités pour le CERTA.

Dans le domaine des publications, le nombre d'avis de sécurité a poursuivi sa progression, avec plus de 760 avis publiés cette année. Ces chiffres ne sont évidemment pas à prendre dans une « logique de record » dont il ne saurait être question. Mais ils sont le reflet du niveau de vulnérabilité des systèmes d'information, ainsi que du niveau de prise en compte de ces vulnérabilités par les constructeurs et éditeurs des produits qu'ils concernent, car le nombre d'alertes quant à lui demeure stable. Des efforts, que nous espérons perçus, ont été entrepris pour améliorer la réactivité de diffusion de ces publications, ainsi que leur contenu : tant au niveau qualitatif, en s'efforçant de mieux qualifier les vulnérabilités pour permettre d'en favoriser l'appréciation de la criticité, que quantitatif, par une rationalisation et une augmentation des produits suivis. À noter, dans ce domaine, la mise en place cette année d'un suivi particulier des vulnérabilités des systèmes industriels (SCADA), avec notamment la mise en place d'un flux RSS spécifique sur le site du CERTA. Un effort qualitatif a également été recherché sur notre bulletin d'actualité hebdomadaire, tant pour en améliorer les thématiques abordées que leur technicité.

Deux notes d'information ont également été publiées pour essayer d'aider nos lecteurs et usagers dans le traitement des attaques en déni de service (CERTA-2012-INF-001), ainsi que les attaques en défiguration de sites (CERTA-2012-INF-002) qui furent encore bien trop nombreuses cette année. Trois notes d'information ont quant à elles été actualisées, dont principalement celle sur les systèmes et logiciels obsolètes (CERTA-2005-INF-003) pour en élargir le spectre de couverture. Les retours de nos lecteurs sont toujours très appréciés pour nous permettre d'orienter nos futurs chantiers d'améliorations.

Dans le domaine opérationnel, 2012 a été une année « riche » en traitement d'incidents de toutes natures. Le nombre des signalements traités par le CERTA ne cesse d'augmenter. Plusieurs raisons en sont la cause :

- la cyberdélinquance et les actes d'espionnage informatiques restent en constante progression ;
- consécutivement, la surveillance des systèmes se renforce, tant au plan technique qu'au plan humain, et avec elle les capacités de détection d'attaques ;
- les coopérations nationales et internationales entre acteurs se structurent et s'intensifient pour favoriser les échanges indispensables pour pouvoir apporter les meilleures réponses possibles aux attaques généralement transnationales ;
- les victimes de l'administration et des opérateurs d'importance vitale (OIV) rendent de plus en plus compte à l'ANSSI des incidents qu'ils rencontrent qui, outre son rôle régalien, est aujourd'hui reconnue comme un partenaire de confiance en mesure d'apporter une aide concrète dans le traitement des incidents auxquels ses usagers sont confrontés.

Une nouvelle fois, il ressort principalement de la diversité des incidents traités par le CERTA que, dans une grande majorité des cas, les attaques auraient pu être évitées par l'application de mesures simples et généralement peu coûteuses d'hygiène informatique, telles l'application régulière des correctifs de sécurité, la mise en place de stratégie de mots de passe robustes, la dissociation des comptes et réseaux d'administration des usages et réseaux d'utilisateurs…

Au plan organisationnel, l'année 2012 aura été marquée par la mise en place de la nouvelle organisation de l'ANSSI. Cette évolution, qui se veut notamment de préfigurer le futur CERT-FR, s'est traduite pour le CERTA par une ventilation de ses missions au sein des différentes composantes du Centre Opérationnel SSI. L'objectif est ici de pouvoir démultiplier les efforts et de professionnaliser encore plus les fonctions dont il est apparu, ces dernières années, qu'elles le nécessitaient pour pouvoir affronter les enjeux auxquels l'ANSSI est confrontée en matière de traitement d'incidents. Ces changements organisationnels ont été accompagnés d'une montée en puissance des effectifs de l'ANSSI, dont une part importante est consacrée au traitement des incidents, donc de sa composante CERTA, et qui se poursuivra sur l'année 2013. À ce titre, nous suggérons à ceux qui en auraient les capacités et qui souhaiteraient nous rejoindre, de consulter notre article dans le présent bulletin d'actualité sur les perspectives de recrutement actuellement offertes par l'ANSSI.

Pour conclure, le CERTA souhaite à tous ses lecteurs une bonne fin d'année 2012 et une bonne année 2013. Que cette nouvelle année qui s'annonce soit marquée de la poursuite des efforts et de la coopération de tous les acteurs qui œuvrent pour assurer la sécurité des systèmes d'information dont ils ont la charge.

# 5 Rappel des avis émis

Dans la période du 21 au 27 décembre 2012, le CERTA a émis les publications suivantes :

- CERTA-2012-ALE-009 : Vulnérabilité dans les pilotes NVidia
- CERTA-2012-AVI-753 : Vulnérabilité dans LemonLDAP::NG
- CERTA-2012-AVI-754 : Vulnérabilités dans IBM Rational Policy Tester et IBM AppScan Entreprise
- CERTA-2012-AVI-755 : Multiples vulnérabilités dans Drupal
- CERTA-2012-AVI-756 : Vulnérabilité dans IBM WebSphere
- CERTA-2012-AVI-757 : Multiples vulnérabilités dans IBM Tivoli
- CERTA-2012-AVI-758 : Multiples vulnérabilités dans IBM InfoSphere Streams
- CERTA-2012-AVI-759 : Multiples vulnérabilités dans VMware
- CERTA-2012-AVI-760 : Vulnérabilités dans CA IdentityMinder
- CERTA-2012-AVI-761 : Multiples vulnérabilités dans Opera
- CERTA-2012-AVI-762 : Multiples vulnérabilités dans les produits IBM Rational
- CERTA-2012-AVI-763 : Vulnérabilité dans IBM Tivoli NetView
- CERTA-2012-AVI-764 : Vulnérabilités dans Tiki Wiki CMS Groupware
- CERTA-2012-AVI-765 : Vulnérabilité dans EMC Data Protection Advisor
- CERTA-2012-AVI-766 : Vulnérabilité dans Symantec Entreprise Security Manager

# Gestion détaillée du document

**28 décembre 2012** version initiale.