Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 05 avril 2013
N° CERTA-2013-ACT-014

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2013-ACT-014

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-2013-ACT-014

1 Sortie de Mozilla Firefox 20 et correctifs associés

La version 20 de Firefox disponible depuis le 2 avril apporte de nouvelles fonctionnalités et surtout une dizaine de correctifs liés à la sécurité du navigateur. Trois de ces vulnérabilités sont critiques, car elles peuvent permettre à un attaquant d'élever ses privilèges locaux ou d'exécuter du code arbitraire sur la machine utilisateur.

À noter que dans le cadre de réseaux d'entreprise où le cycle de déploiement de versions logicielles est plus long, il est possible de s'appuyer sur les éditions disposant d'un support étendu (ESR, "Extended Support Release"). La maintenance des éditions ESR est limitée uniquement aux vulnérabilités qui présentent des risques importants : aucune nouvelle fonctionnalité introduite dans les dernières versions du projet n'est répercutée sur ces versions ESR. La dernière version 17.0.5 de Firefox intègre également les derniers correctifs évoqués supra.

Le CERTA recommande l'application au plus tôt de ces correctifs.

1.1 Documentation

- Mozilla Firefox - ESR : Vue d'ensemble
  http://www.mozilla.org/fr/firefox/organizations/faq/
- Mozilla Foundation - Security Advisories
  http://www.mozilla.org/security/announce/

2 Dénis de services par amplification DNS

Fin mars 2013 une organisation de lutte contre le spam a subit une attaque de type déni de service se basant sur le protocole DNS.

DNS est un protocole majoritairement transporté par la couche UDP (User Datagram Protocol), ce qui l'expose au risque d'usurpation de l'émetteur. En effet, UDP étant un protocole « non connecté », l'adresse IP ne peut être considérée comme un moyen d'identification fiable.

Les requêtes DNS de type « AXFR » et « IXFR » sont particulièrement utilisées par les attaques par dénis de services. Elles permettent de transférer la configuration de zones vers un autre serveur DNS. Si un serveur DNS accepte des requêtes de transfert de zones en UDP sans restriction sur les adresses IP émettrices une attaque par amplification de trafic est alors possible.

Un attaquant peut usurper l'adresse IP de la victime et demander un transfert de zones. La victime recevra alors la réponse du serveur DNS qui sera largement plus volumineuse que la requête envoyée par l'attaquant. Il faut noter que les serveur DNS sur Internet possèdent généralement une bande passante assez volumineuse, ce qui augmente d'autant les risques de saturation de la victime.

Il est également possible, au moyen de requêtes récursives, d'amplifier la taille des réponses d'un serveur DNS s'il ne possède pas de restrictions relatives aux demandeurs. Comme précédemment un attaquant peut usurper l'adresse IP de la victime, rediriger le trafic et ainsi la saturer.

La note CERTA-2012-INF-001 propose un ensemble de mesures préventives à mettre en place afin de limiter les risques d'utilisations malveillantes. Le CERTA recommande également aux administrateurs de configurer leurs serveurs DNS pour n'accepter les requêtes de transfert de zones que depuis une liste blanche. Dans le même esprit il est conseillé de désactiver le mode récursif sur les serveurs DNS accessibles depuis Internet.

Documentation

– Note d'information CERTA-2012-INF-001 :
http://www.certa.ssi.gouv.fr/site/CERTA-2012-INF-001/index.html

3 Stockage de documents en ligne sur Internet

Les services de stockage en ligne de documents sur Internet, permettent de conserver ou sauvegarder des quantités de donnes importantes. La sécurité de ces données dépend des protections mises en œuvre par l'hébergeur.

Récemment, des chercheurs ont mis en évidence des lacunes dans le contrôle d'accès des données stockées sur les serveurs de stockage en ligne « Amazon S3 ». Le simple fait de connaître ou de deviner le lien du répertoire de stockage (via un moteur de recherche ou par une recherche exhaustive) offre la possibilité à une personne tierce de consulter les documents à l'insu de leur propriétaire.

Cette vulnérabilité démontre une nouvelle fois l'attention particulière qu'il convient de porter aux services de stockage en ligne et en particulier, les mécanismes de sécurité mis en œuvre par l'éditeur de la solution : authentification des accès, chiffrement des données, etc.

De manière plus générale, il est rappelé que des risques inhérents à l'externalisation sont :

– les risques liés à la perte de maîtrise de la confidentialité de ses informations;
– les risques liés aux interventions à distance;
– les risques liés à l'hébergement mutualisé.

Le guide de l'ANSSI sur l'externalisation des systèmes d'information propose des recommandations visant à pallier ces risques (cf. documentation).

En outre, pour limiter les risques de diffusion fortuites d'informations sensibles, le CERTA recommande de veiller à n'utiliser que des services de stockage en ligne qui garantissent la mise en place de contrôle d'accès sur les espaces de stockage, et de chiffrer en amont tout document sensible qui devrait être stocké en ligne.

Documentation

– Guide d'externalisation des systèmes d'information :
http://www.ssi.gouv.fr/IMG/pdf/2010-12-03_Guide_externalisation.pdf
– Bulletin d'actualité CERTA-2013-ACT-006 :
http://www.certa.ssi.gouv.fr/site/CERTA-2013-ACT-006/

4 Rappel des avis émis

Dans la période du 29 mars au 4 avril 2013, le CERTA a émis les publications suivantes :

– CERTA-2013-AVI-208 : Vulnérabilité dans VMware ESX et ESXi
– CERTA-2013-AVI-209 : Vulnérabilité dans HP ProCurve
– CERTA-2013-AVI-210 : Vulnérabilité dans ISC BIND
– CERTA-2013-AVI-211 : Multiples vulnérabilités dans ZENworks
– CERTA-2013-AVI-212 : Multiples vulnérabilités dans Skype
– CERTA-2013-AVI-213 : Vulnérabilité dans IBM InfoSphere
– CERTA-2013-AVI-214 : Multiples vulnérabilités dans les produits Mozilla
– CERTA-2013-AVI-215 : Multiples vulnérabilités dans les produits ESR Mozilla
– CERTA-2013-AVI-216 : Vulnérabilité dans les pilotes NVIDIA

- CERTA-2013-AVI-217 : Vulnérabilité dans Samba
- CERTA-2013-AVI-218 : Multiples vulnérabilités dans le système SCADA Wind River VxWorks
- CERTA-2013-AVI-219 : Multiples vulnérabilités dans le noyau Linux d' Ubuntu
- CERTA-2013-AVI-220 : Multiples vulnérabilités dans Opera
- CERTA-2013-AVI-221 : Multiples vulnérabilités dans PostgreSQL

Gestion détaillée du document

05 avril 2013 version initiale.