Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 31 mai 2013
N° CERTA-2013-ACT-022

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2013-ACT-022

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-022

1 De l'utilité des cartographies et plans réseaux dans le cadre du traitement d'incident

Récemment, le CERTA a été amené à traiter une suspicion d'incident sur une possible exfiltration de données vers l'Internet via un canal de communication chiffré.

Après investigation, il s'est avéré que le serveur de destination du flux suspect était en fait un serveur interne qui utilisait une adresse IP routable sur l'Internet.

L'engagement de ressources dans les investigations en traitement d'incident est coûteux. En l'espèce cet investissement aurait pu être évité :

- en respectant les règles d'adressage des réseaux locaux telles que prescrites dans la RFC 1918 ;
- en disposant d'un plan d'adressage et des flux supervisés tenu à jour tel que prescrit par la règle numéro 1 du guide d'hygiène informatique proposé par l'ANSSI.

Le CERTA encourage au respect de ces prescriptions afin d'optimiser le traitement d'incident en cas de compromission ou de suspicion de compromission.

Documentation

- Plages d'adressage privées (page 3) :
  http://tools.ietf.org/html/rfc1918
- Guide d'hygiène informatique :
  http://www.ssi.gouv.fr/IMG/pdf/guide_hygiene_informatique_anssi.pdf

2 LaFoSec: Sécurité des langages fonctionnels

L'ANSSI a lancé l'étude LaFoSec sur les langages fonctionnels et notamment le langage OCaml.

Cette étude avait pour objectif principal d'étudier l'adéquation des langages fonctionnels pour le développement d'applications de sécurité et de proposer le cas échéant des recommandations.

Cette étude a donné lieu à la livraison de 5 rapports, qui ont été validés par les laboratoires de l'ANSSI :

- état des lieux des langages fonctionnels ;
- analyse des langages OCaml, F# et Scala ;
- modèles d'exécution de OCaml ;
- outils associés au langage OCaml ;

– recommandations relatives à l'utilisation du langage OCaml et à l'installation et la configuration des outils associés.

Ces documents sont accessibles à l'adresse :

http://www.ssi.gouv.fr/fr/anssi/publications/publications-scientifiques/autres-publications/lafosec-securite-et-langages-fonctionnels.html

3 Rappel des avis émis

Dans la période du 24 au 30 mai 2013, le CERTA a émis les publications suivantes :

– CERTA-2013-AVI-325 : Multiples vulnérabilités dans RT
– CERTA-2013-AVI-326 : Multiples vulnérabilités dans Apple Quicktime
– CERTA-2013-AVI-327 : Multiples vulnérabilités dans le système SCADA Siemens Scalance X200 IRT
– CERTA-2013-AVI-328 : Multiples vulnérabilités dans le noyau Linux de Ubuntu
– CERTA-2013-AVI-329 : Vulnérabilité dans SPIP
– CERTA-2013-AVI-330 : Vulnérabilité dans SpiderLabs ModSecurity
– CERTA-2013-AVI-331 : Multiples vulnérabilités dans EMC RSA Authentication Manager
– CERTA-2013-AVI-332 : Vulnérabilité dans Apache
– CERTA-2013-AVI-333 : Vulnérabilité dans IBM WebSphere
– CERTA-2013-AVI-334 : Multiples vulnérabilités dans Apache Tomcat

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

– CERTA-2013-ALE-005-002 : Vulnérabilité dans le noyau Linux (ajout correctif SUSE)

Gestion détaillée du document

31 mai 2013 version initiale.