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 juin 2013
N° CERTA-2013-ACT-026

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2013-ACT-026

1 Référentiel d'exigences applicable aux prestataires d'audit de la SSI

L'ANSSI a publié le 21 juin la version définitive du référentiel d'exigences applicable aux prestataires d'audit de la sécurité des systèmes d'information (PASSI).

Ce référentiel a vocation à permettre la qualification des prestataires d'audit de la SSI et est destiné à être intégré dans la prochaine version du référentiel général de la sécurité (RGSv2). Les activités d'audit décrites sont :

- audit d'architecture ;
- audit de configuration ;
- audit de code source ;
- tests d'intrusion ;
- audit organisationnel et physique.

Enfin, des recommandations permettant d'aider les autorités administratives à exprimer leurs besoins d'audit et des exemples de compétences techniques, théoriques et pratiques dont doit disposer un prestataire d'audit pour être qualifié, sont rassemblés en annexe du document

Documentation

- Publication du référentiel d'exigences applicable aux prestataires d'audit de la SSI :
  http://www.ssi.gouv.fr/fr/menu/actualites/publication-du-referentiel-d-exigences-applicable-aux-prestataires-d-audit-de.html

2 Escroquerie en ligne portant le logo de l'ANSSI : mise en place d'un numéro d'urgence

De nombreux internautes sont actuellement victimes d'un code malveillant usurpant les couleurs de l'ANSSI, qui bloque leur ordinateur dans l'attente du règlement d'une rançon. Afin d'aider les victimes de ce rançongiciel, l'ANSSI a mis en place un numéro d'urgence (01.71.76.85.98) avec un répondeur pour leur décrire la marche à suivre en cas de compromission.

Aucune entité gouvernementale française ne bloquerait un ordinateur pour inciter au paiement d'une amende et ne forcerait un internaute à la régler par l'intermédiaire d'un site non gouvernemental.

Comme de nombreux autres organismes officiels, l'ANSSI est régulièrement invoquée dans ce type de tentative de fraude. Il y a un an le CERTA avait évoqué dans son bulletin CERTA-2012-ACT-026 une affaire similaire.

L'ANSSI rappelle que face à ce type d'escroquerie, les utilisateurs ne doivent surtout pas payer la somme demandée. Pour désinfecter leur poste, les utilisateurs doivent faire appel à un technicien informatique et s'appuyer sur le tutoriel mentionné dans la section documentation. Pour les utilisateurs qui se seraient fait duper, l'ANSSI recommande de faire opposition au paiement et de déposer plainte auprès des services de police ou de gendarmerie.

Documentation

- Publication de l'ANSSI concernant le rançongiciel :
  http://www.ssi.gouv.fr/fr/menu/actualites/attention-arnaque-en-ligne-portant-le-logo-de-l-anssi.html
- Article présentant les actions à mener en cas de d'escroquerie :
  http://blog.crimenumerique.fr/2012/05/17/les-rancongiciels-sont-toujours-tres-actifs/
- Bulletin d'actualité CERTA-2012-ACT-026 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-ACT-026/CERTA-2012-ACT-026.html

3 Rappel des avis émis

Dans la période du 21 au 27 juin 2013, le CERTA a émis les publications suivantes :

- CERTA-2013-AVI-369 : Multiples vulnérabilités dans Xen
- CERTA-2013-AVI-370 : Multiples vulnérabilités dans VideoLan VLC
- CERTA-2013-AVI-371 : Vulnérabilité dans INDEPNET GLPI
- CERTA-2013-AVI-372 : Vulnérabilité dans Hewlett-Packard iLO
- CERTA-2013-AVI-373 : Vulnérabilité dans libcurl
- CERTA-2013-AVI-374 : Multiples vulnérabilités dans les produits Mozilla
- CERTA-2013-AVI-375 : Multiples vulnérabilités dans le noyau Linux de Mandriva
- CERTA-2013-AVI-376 : Multiples vulnérabilités dans Cisco Content Security Management Appliance
- CERTA-2013-AVI-377 : Multiples vulnérabilités dans Cisco Email Security Appliance
- CERTA-2013-AVI-378 : Multiples vulnérabilités dans Cisco Web Security Appliance
- CERTA-2013-AVI-379 : Vulnérabilité dans Cisco ASA Next-Generation Firewall

Gestion détaillée du document

28 juin 2013 version initiale.