Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 27 septembre 2013
N° CERTA-2013-ACT-039

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2013-ACT-039

1 - La sécurité des réseaux déconnectés

Le CERTA est régulièrement amené à traiter des incidents sur des réseaux déconnectés. Ces réseaux n'ont pas de lien physique vers l'Internet, généralement dans le but de se protéger des risques de vol de données sensibles. Cette déconnexion est aussi requise, par exemple, dans le cas de réseaux hébergeant des données classifiées et/ou sensibles.

Si l'absence de connexion à Internet est une mesure efficace contre certaines menaces, elle ne protège pas à elle seule un réseau et ne saurait se substituer à l'application scrupuleuse d'une défense en profondeur.

En effet, les menaces pesant sur les réseaux connectés pèsent tout autant sur les réseaux déconnectés. En 2008, le ver Conficker exploitait déjà plusieurs vulnérabilités lui permettant de se transmettre aussi bien sur les réseaux connectés que déconnectés. Ces méthodes de propagation à la fois en ligne et hors ligne ont depuis été vues dans d'autres attaques agressives : Par exemple Stuxnet, conçu pour se transmettre jusqu'à des réseaux déconnectés et y effectuer en autonomie des actions destructrices.

La panoplie des mesures de défense en profondeur doit donc être appliquée à ces réseaux afin d'en protéger les ressources sensibles qu'ils hébergent.

Malheureusement, lors de ses investigations, le CERTA est amené à constater que l'hygiène SSI des réseaux déconnectés est très souvent inférieure à celle des réseaux connectés voire négligée. Par exemple la fréquence de mises à jour des logiciels est, au mieux, sporadique (...quand elle existe). De même, la présence de systèmes d'exploitation ou d'applications obsolètes est régulièrement constatée. Les politiques de mots de passe sont faibles ou inappliquées... On peut regretter que la décision de protéger des réseaux sensibles en les déconnectant puisse entraîner un relâchement sur les autres mesures de protection alors que, justement, l'objectif était d'assurer une protection maximale.

Pour mémoire, les points importants à prendre en compte pour la sécurité d'un réseau déconnecté sont :

- Les sas ou « Machines blanches » :
  Ces ordinateurs sont désignés comme points d'entrée uniques du réseau déconnecté. Ils pourront ainsi héberger des logiciels particuliers pour suivre les imports/exports du réseau : anti-virus, contrôle de clefs USB, journalisation des clefs et des fichiers copiés. Pour être efficace, il convient d'y installer un anti-virus distinct de celui déployé sur le reste du réseau, et évidemment de le maintenir à jour. À ces ordinateurs sas sont connectés beaucoup de supports amovibles. Un risque majeur est qu'une fois compromis, ils peuvent se transformer en foyer d'infection. Pour atténuer ce risque, on envisagera soit une remasterisation régulière des machines sas, soit l'usage d'un système d'exploitation sur un support en lecture seule (livecd Linux, Windows PE).
- La supervision :
  Un réseau déconnecté ne peut s'appuyer sur l'architecture de supervision déployée dans le reste de l'entreprise (journaux, remontée d'alertes). Sa supervision doit donc être assurée indépendamment avec le coût en logiciels et en moyens humain afférent. Typiquement, la surveillance des tentatives d'accès à des adresses Internet depuis ce réseau sera aussi particulièrement utile à surveiller. Celle-ci passera, par exemple, par

l'installation d'une fausse passerelle et la surveillance des résolutions DNS (par exemple par INetSim). Une fois écartées les tentatives légitimes (de certains logiciels pour se mettre à jour ou avec des fonctionnalités en ligne), l'apparition de tentatives issues d'un logiciel malveillant sera aisément détectable.

– Les mises à jour :
  Une infrastructure de déploiement des mises à jour de l'antivirus, des systèmes d'exploitation et des logiciels déployés (VM Java, suites Office, Adobe, etc...) doit également être mise en place.

Au regard de leur particularité technique et de la sensibilité des informations qu'ils hébergent, le CERTA recommande d'apporter une attention particulière aux réseaux déconnectés et de s'assurer qu'ils disposent d'un haut degré d'hygiène SSI.

Documentation

– Guide d'hygiène SSI :
  http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-du-poste-de-travail-et-des-serveurs/l-anssi-publie-la-version-finalisee-du-guide-d-hygiene-informatique.html

2 - Injections SQL à l'aide du logiciel HAVIJ

Les injections SQL au sein de sites Internet ou de solutions Web font partie des failles applicatives les plus fréquemment exploitées. Celles-ci sont déclenchées par l'exploitation de failles applicatives ou de paramètres mal validés par le code de l'application web. Le fonctionnement des injections SQL est détaillé dans la note d'information CERTA-2004-INF-001.

De nombreux outils tel que le logiciel HAVIJ, développé par ITSECTEAM, sont disponibles sur l'Internet et permettent de détecter automatiquement les pages web vulnérables et de les exploiter. Cette application, simple d'utilisation et disponible en version gratuite, est à l'origine de nombreux signalements effectués par le CERTA. En effet, si le site est vulnérable, HAVIJ permet en générant des requêtes SQL spécifiques de lire et modifier frauduleusement les informations stockées au sein des bases de données voire d'exécuter des commandes système.

La correction de ces vulnérabilités passe par un examen approfondi du code source et plus particulièrement par une validation fine (typage fort, suppression des meta-caractères, requêtes préparées...) des informations envoyées par le client au Système de Gestion des Bases de Données (SGBD) notamment via les champs de formulaires, cookies, paramètres d'URL ou toute information manipulable par le visiteur du site.

La mise à jour des gestionnaires de contenu (comme Joomla!, Wordpress, Drupal, etc.) et des greffons installés participera à limiter la surface d'attaque. Lorsque cela est possible, le déploiement d'un pare-feu applicatif (WAF) permet le filtrage de certaines requêtes, reconnues comme malveillantes, transmises au serveur. De même, en cas d'erreur dans le traitement de la requête il est préférable de ne pas retourner la commande traitée afin de ne pas fournir d'élément utile à l'attaquant, en désactivant toutes les options de débogage sur les sites en production.

L'application d'algorithmes cryptographiques sur les informations sensibles présentes au sein de la base de données (mots de passe, données personnelles...) et une gestion stricte des droits des utilisateurs de la base permettront de limiter les effets d'une éventuelle compromission.

La détection de l'exploitation d'une vulnérabilité SQL passe par la mise en place d'une politique de journalisation et un examen régulier des journaux générés. La recherche de marqueurs spécifiques au sein des journaux du serveur web peut s'avérer utile (liste non exhaustive) :

– terme `havij` présent dans le user-agent (ce user-agent par défaut est toutefois modifiable par l'attaquant)
– requêtes contenant les termes `0x31303235343830303536` ou `0x7233646D3076335F68766A5F696E6A656374696F6E`
– requêtes contenant des commandes SQL classiques `UNION`, `SELECT`, `CONCAT`, `JOIN`, etc.
– requêtes anormales par leur longueur, leur nombre ou l'utilisation de codages particuliers

Cependant, l'identification peut s'avérer délicate. En effet, le contenu exact des requêtes adressées à l'aide de la méthode `POST` ne peut être extrait des journaux du serveur web. L'examen des journaux liés au SGBD (journal des requêtes et journal des requêtes lentes) ou du pare-feu applicatif peut permettre de relever des informations utiles sur une éventuelle tentative de compromission.

S'il apparaît qu'une faille SQL a été exploitée il convient d'analyser les fichiers de journalisation et d'identifier la page et la variable impliquées afin de durcir le processus de validation des données transmises par l'utilisateur. Une relecture attentive du code permettra de s'assurer que cette vulnérabilité n'est pas présente sur d'autres pages.

Tous les mots de passe qui auraient pu être compromis devront être modifiés dans les plus brefs délais et la gestion des droits des utilisateurs du SGBD révisée si nécessaire.

Afin d'aviser rapidement les responsables de sites Internet vulnérables à ce type d'attaque, le CERTA rappelle qu'il convient de tenir à jour les informations de contact des bases `WHOIS` tout comme l'enregistrement SOA de la zone DNS associée au site. Les informations de contacts techniques présentes sur les sites Internet doivent également être facilement identifiables et les boîtes de messagerie correspondantes consultées régulièrement. Les éléments pouvant permettre d'identifier l'auteur de l'attaque et de caractériser ses actes devront être conservés pour pouvoir être communiqués aux services de police dans le cadre d'un éventuel dépôt de plainte.

Documentation

- Note d'information du CERTA - Sécurité des applications Web et vulnérabilité de type injection de données :

  http://www.certa.ssi.gouv.fr/site/CERTA-2004-INF-001/index.html
- Note technique ANSSI - Recommandations pour la sécurisation des sites web :
  http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-des-applications-web/recommandations-pour-la-securisation-des-sites-web.html
- Note d'information du CERTA - Les bons réflexes en cas d'intrusion sur un système d'information :
  http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-002/index.html
- Bulletin d'actualité CERTA-2012-ACT-045 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-ACT-045/
- Bulletin d'actualité CERTA-2011-ACT-045 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2011-ACT-045/

3 - Mises à jour des navigateurs et de leurs greffons

Le CERTA constate régulièrement que la proportion de navigateurs et de greffons obsolètes dans les parcs informatiques est très importante. L'exploitation de vulnérabilités dans ces logiciels est l'un des principaux vecteurs d'attaque. Il est donc primordial de maintenir le parc à jour, afin de se prémunir des attaques les plus courantes.

Pour ce faire, différentes mesures peuvent être mises en place :

- certains logiciels ont deux branches de développement. L'une, destinée au grand public, apporte régulièrement de nouvelles fonctionnalités. L'autre, pour les entreprises, n'est mise à jour que pour intégrer des correctifs de sécurité. Lorsque c'est possible, cette dernière est donc à privilégier pour faciliter la gestion des mises à jour, car leur publication est moins fréquente et a potentiellement moins d'impact d'intégration dans le SI ;
- la difficulté majeure pour le maintien à jour d'un parc est la capacité de connaître les versions installées sur chaque poste. A cette fin, un logiciel d'inventaire de parc peut être installé ;
- pour s'assurer que les navigateurs et les greffons obsolètes ne puissent pas se connecter sur Internet, l'analyse et le blocage des *user-agents* non désirés au niveau du relai HTTP est la mesure la plus efficace. Elle permet d'identifier rapidement les postes concernés tout en les protégeant.
- enfin, lorsque les greffons ne sont pas nécessaires, le CERTA recommande leur désinstallation (cf. bulletin d'actualité n°24 pour Java).

Documentation

- Règles 6, 7 et 16 du guide d'hygiène informatique :
  http://www.ssi.gouv.fr/IMG/pdf/guide_hygiene_informatique_anssi.pdf
- Bulletin d'actualité n°24 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-ACT-024/

4 - Site web du CERTA - Nouvelle fonctionalité

Afin de répondre à une demande de ses usagers, une nouvelle fonctionalité à été ajoutée sur le site web du CERTA permettant de télécharger une archive au format tar de l'ensemble des AVIS émis par le CERTA par année, au format txt et pdf. Cette fonctionalité est accessible via une icone située dans le menu a proximité du lien vers les documents de l'année en cours et des liens vers les archives.

Le CERTA recommande fortement à ses visiteurs d'utiliser cette nouvelle fonctionalité à la place des scripts jusqu'alors employés. En effet, l'utilisation de tels scripts (sans limite du nombre de requêtes vers le site du CERTA) pourraient entrainer une mise en lise noire de l'adresse IP source et lui interdire l'accès au site.

5 - Rappel des avis émis

Dans la période du 20 au 26 septembre 2013, le CERTA a émis les publications suivantes :

- CERTA-2013-AVI-538 : Multiples vulnérabilités dans GLPI
- CERTA-2013-AVI-539 : Vulnérabilité dans F5 BIG-IP APM
- CERTA-2013-AVI-540 : Multiples vulnérabilités dans Moodle
- CERTA-2013-AVI-541 : Multiples vulnérabilités dans Apple TV
- CERTA-2013-AVI-542 : Multiples vulnérabilités dans Blue Coat
- CERTA-2013-AVI-543 : Multiples vulnérabilités dans Oracle Solaris
- CERTA-2013-AVI-544 : Multiples vulnérabilités dans Cisco IOS
- CERTA-2013-AVI-545 : Multiples vulnérabilités dans le noyau Linux de Mandriva

Gestion détaillée du document

27 septembre 2013 version initiale.