Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 26 octobre 2012
N° CERTA-2012-ACT-043

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2012-ACT-043

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-043`

1 Attaques sur des accès SSH et RDP

La prise de contrôle d'une machine ayant un accès distant de type SSH ou RDP activé est souvent causée par un défaut de configuration ou la présence d'une vulnérabilité.

L'existence de nombreux équipements vulnérables accessibles depuis l'Internet attire toute l'attention des attaquants pour prendre le contrôle d'accès distants non protégés ou mal configurés. Un examen de journaux de connexions SSH sur une machine connectée à l'Internet permet souvent de mettre rapidement en évidence de nombreuses tentatives d'attaques par dictionnaire.

Ces attaques, souvent d'un niveau technique simple lorsqu'elles réussissent, permettent de prendre le contrôle de nombreuses machines. Menées à grande échelle, elle permettent à des organisations douteuses de mettre en vente facilement ces accès pour des sommes très modiques. Il est aujourd'hui courant de trouver sur l'Internet ce genre d'offre, très diversifiée et qui peut être sélectionnée selon différents critères : bande passante, puissance de calcul ou encore le nom de la société visée !

Il est primordial, pour une organisation, d'établir une liste exhaustive de ces accès distants et d'évaluer si leur activation est indispensable. Cette liste doit comprendre, en plus des machines clientes et des serveurs, l'ensemble des équipements réseau.

Si un accès distant doit être impérativement activé, le CERTA recommande la mise en place de mesures de protection et de surveillance particulières telles que :

- le filtrage qui permet de limiter l'accès à une liste déterminée d'IP, et qui est une solution simple mais efficace ;
- les choix des mots de passe et/ou des clés qui doivent être suffisament longs et robustes ;
- la surveillance et la configuration des journaux d'évènements, afin de remonter toute alerte et permettre, en cas d'attaque réussie, d'évaluer rapidement les impacts sur le SI.

2 Services mandataires d'administration à distance

Le 12 octobre 2012, dans le bulletin d'actualité CERTA-2012-ACT-041, nous signalions la publication par l'ANSSI de la note technique de recommandations de sécurité relatives à la télé-assistance. Cette note donne des conseils pour la mise en place d'outils de télé-administration de postes, et présente les risques de sécurité des principales solutions logicielles.

Dans ce registre, certaines sociétés fournissent des services d'administration de poste à distance qui fonctionnent de la manière suivante : un logiciel est installé sur le poste à administrer et se connecte à un serveur mandataire

distant sur l'Internet. Il est ensuite possible, avec un simple navigateur Web ou un logiciel approprié, de contacter ce serveur mandataire pour obtenir des fonctions d'administration, comme par exemple un affichage déporté du bureau du poste à administrer.

De tels mécanismes présentent plusieurs problèmes potentiels, notamment lorsque le poste à administrer est situé au sein du système d'information, et que le poste client se trouve à l'extérieur :

1. confidentialité des données : le serveur mandataire peut intercepter toutes les données en transit entre le poste client et le poste à administrer (par exemple les frappes clavier de l'opérateur) ;
2. augmentation de l'exposition du système d'information : si le client ou la base de données du serveur d'authentification sont compromis, un utilisateur malveillant pourrait compromettre le poste à administrer en utilisant les secrets d'authentification dérobés pour s'y connecter ;
3. contournement de la polititique de sécurité : un administrateur pourra difficilement filtrer et contrôler les flux de communication avec les serveurs mandataires, car ces outils encapsulent souvent leur trafic dans un protocole généralement autorisé en sortie vers l'Internet, comme HTTPS. Un attaquant ayant préalablement intercepté les secrets d'authentification jouit alors d'une porte d'entrée difficilement contrôlable sur le SI.

Le CERTA recommande de sensibiliser les administrateurs et utilisateurs aux risques liés à l'installation et l'utilisation de ces types d'outils d'administration à distance, et éventuellement à en interdire l'usage.

Documentation

- Bulletin d'actualité CERTA-2012-ACT-041 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-ACT-041/
- Recommandations de sécurité relatives à la télé-assistance :
  http://www.ssi.gouv.fr/IMG/pdf/NP_Teleassistance_NoteTech.pdf

3 Préparer sa migration vers Java 7

Le 19 septembre 2012, Oracle a publié une note de rappel sur le support des versions Java. À partir de février 2013, il n'y aura plus de correctif de sécurité et de mise à jour pour Java SE version 6. En revanche, une extension du support jusqu'à décembre 2016 est possible avec l'offre « Oracle SE Commercial Offering ». La dernière version stable (version 7) ne sera plus mise à jour à partir de juillet 2014.

Le CERTA ne peut qu'inciter les administrateurs et les développeurs Java version 6 de commencer à préparer leur migration vers Java version 7. Le CERTA tient à souligner qu'il ne reste que 4 mois pour mettre à jour les applications métier vers Java version 7, et qu'à partir de février 2013, il n'y aura plus aucun correctif de sécurité.

Le CERTA recommande la plus grande vigilance sur la date d'échéance des versions des produits utilisés, afin de pouvoir anticiper les migrations nécessaires pour continuer à disposer des produits tenus à jour par les éditeurs.

D'une manière générale, le CERTA recommande d'utiliser systématiquement la dernière version stable des produits et de veiller à la bonne mise à jour des correctifs de sécurité.

Documentation

- Note d'Oracle du 19 septembre 2012 :
  http://www.oracle.com/technetwork/java/javase/eol-135779.html

4 Rappel des avis émis

Dans la période du 19 au 25 octobre 2012, le CERTA a émis les publications suivantes :

- CERTA-2012-AVI-590 : Multiples vulnérabilités dans Drupal
- CERTA-2012-AVI-591 : Vulnérabilités dans CA ARCserve Backup
- CERTA-2012-AVI-592 : Multiples vulnérabilités dans IBM DB2 QMF
- CERTA-2012-AVI-593 : Vulnérabilité dans IBM WebSphere Message Broker
- CERTA-2012-AVI-594 : Multiples vulnérabilités dans IBM XIV Storage System
- CERTA-2012-AVI-595 : Multiples vulnérabilités dans les composants Java de HP-UX
- CERTA-2012-AVI-596 : Vulnérabilité dans McAfee Firewall Enterprise

- CERTA-2012-AVI-597 : Vulnérabilité dans IBM AIX
- CERTA-2012-AVI-598 : Vulnérabilité dans IBM DataQuant et IBM DB2
- CERTA-2012-AVI-599 : Multiples vulnérabilités dans Adobe Shockwave Player
- CERTA-2012-AVI-600 : Vulnérabilité dans F5 FirePass
- CERTA-2012-AVI-601 : Multiples vulnérabilités dans HP-UX
- CERTA-2012-AVI-602 : Vulnérabilité dans AIX BIND
- CERTA-2012-AVI-603 : Vulnérabilité dans ISC BIND

Gestion détaillée du document

26 octobre 2012 version initiale.