Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 07 décembre 2012
N° CERTA-2012-ACT-049

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2012-ACT-049

1 Sécurité des autocommutateurs

Les attaques envers les autocommutateurs téléphoniques (PABX) reportés au CERTA sont actuellement en augmentation. Les autocommutateurs sont des cibles de choix pour les attaquants en raison du faible niveau de sécurité généralement constaté sur ces équipements. Pourtant, la compromission d'un autocommutateur peut avoir des conséquences importantes pour la victime (facturation d'appels illégitimes, usurpation d'identité, écoute téléphonique, déni de service, etc.). Une configuration laxiste de l'autocommutateur est souvent la cause de la réussite de telles attaques.

Le CERTA recommande donc de prêter une attention particulière à la sécurité de ces équipements, en appliquant au minimum les mesures suivantes :

- vérifier le contrat de maintenance ou d'externalisation de l'exploitation souvent associés à l'équipement. Ce contrat doit comprendre une surveillance du système par le prestataire (journaux, relevés d'incidents, etc.) et des protocoles de transmissions d'informations et d'alerte ;
- intégrer l'autocommutateur au référentiel de sécurité, au même titre que les autres composants du système d'information ;
- qualifier puis appliquer les derniers correctifs de sécurité du constructeur ;
- appliquer une politique de mots de passe forts pour l'administration de l'autocommutateur ;
- vérifier la bonne configuration des droits des utilisateurs, notamment pour l'autorisation d'appels à l'international ;
- initialiser les codes d'accès des boites vocales des utilisateurs à des valeurs autres que celles par défaut et demander aux utilisateurs déjà enregistrés de changer leur code. Si l'autocommutateur dispose d'une fonctionnalité permettant d'empêcher la configuration de codes d'accès triviaux (0000, 1234, etc.) celle-ci doit-être activée ;
- désactiver la fonction DISA (*Direct Inward System Access* : fonctionnalité permettant à un utilisateur externe d'accéder aux fonctionnalités du commutateur normalement accessibles uniquement en interne) si elle n'est pas nécessaire ou, dans le cas contraire, limiter les services de l'autocommutateur accessibles via cette fonction et les personnes pouvant accéder à ce service.

Il est également vivement recommandé de rechercher la présence d'anomalies pouvant être le signe d'une compromission d'un autocommutateur. Ces anomalies peuvent être une facturation téléphonique d'un montant inhabituel ou des appels vers des destinations étrangères sans rapport avec l'activité professionnelle.

2 Les imprimantes en réseau, des éléments à ne pas négliger

Les imprimantes réseau doivent être considérées comme des systèmes complexes à part entière. Les services et les protocoles pris en charge sont nombreux (*HTTP, FTP, AppleTalk, LPD, IPP, Telnet, SLP, Bonjour, SNMP*, ...).

Ces fonctionnalités ne sont toutefois pas exempts de vulnérabilités. Nous pouvons citer en exemple un avis de l'US-CERT concernant des vulnérabilités dans des imprimantes Samsung (cf. section Documentation). Cela démontre également qu'il est difficile d'identifier les dépendances logicielles du système et de déterminer si des correctifs ou contournements doivent être appliqués. De plus, la signature des micrologiciels (*firmwares*) par les constructeurs n'est pas systématique : dans le cas où l'imprimante est mal configurée, elle peut donc être exposée à un potentiel remplacement de son micrologiciel par un attaquant. Les impacts d'une compromission, qu'ils soient dûs à une mauvaise configuration ou à l'utilisation d'une vulnérabilité sont nombreux :

- déni de service (modification de la configuration ou du micrologiciel) ;
- fuite d'information (modification du micrologiciel, utilisation abusive d'une fonctionnalité de réimpression, accès physique ou via le réseau au stockage interne de l'imprimante, capture d'un flux non chiffré vers l'imprimante, ...) ;
- infections de postes de travail, serveurs et autres périphériques (modification du micrologiciel) ;
- persistance d'un attaquant après la compromission d'un système d'information sur une imprimante compromise (modification du micrologiciel) ;
- destruction du matériel (surchauffe, incendie) (modification du micrologiciel) ;
- gaspillage de consommables (modification de la configuration ou du micrologiciel).

Les mesures de protections envisageables peuvent être :

- la désactivation des services inutiles ;
- la mise en place d'une configuration adaptée (mot de passe, restrictions d'utilisation et d'accès) ;
- la mise en place d'un cloisonnement des réseaux d'impression en filtrant l'accès à l'imprimante et à ses services pour les utilisateurs concernés ;
- la mise en place d'un serveur d'impression centralisé (l'imprimante n'acceptant que les requêtes émises par ce serveur et mise en place de flux chiffrés lors de l'impression entre le serveur et les clients).

Des limitations peuvent exister lorsque des contrats de service pour les imprimantes sont souscrits. En effet, il est malheureusement courant de voir que les administrateurs sont contraints de laisser communiquer l'imprimante avec un serveur sur l'Internet pour des raisons de maintenance (la mise en place d'un filtrage pourrait alors limiter voire annuler la garantie).

Le CERTA recommande de prêter attention aux mises à jour et aux correctifs de sécurité que les constructeurs mettent à disposition et de les appliquer. Les restrictions apportées par des contrats de services, ainsi que leurs impacts sur le système d'information doivent également être pris en compte.

Documentation

- Avis de sécurité 281284 de l'US-CERT :
  http://www.kb.cert.org/vuls/id/281284

3 Rappel des avis émis

Dans la période du 30 novembre au 06 décembre 2012, le CERTA a émis les publications suivantes :

- CERTA-2012-ALE-007 : Vulnérabilité dans MySQL
- CERTA-2012-AVI-690 : Multiples vulnérabilités dans Google Chrome
- CERTA-2012-AVI-691 : Multiples vulnérabilités dans Apple TV
- CERTA-2012-AVI-692 : Multiples vulnérabilités dans Wireshark
- CERTA-2012-AVI-693 : Multiples vulnérabilités dans IBM Lotus Symphony
- CERTA-2012-AVI-694 : Multiples vulnérabilités dans IBM DOORS Web Access
- CERTA-2012-AVI-695 : Vulnérabilité dans IBM WebSphere Message Broker
- CERTA-2012-AVI-696 : Multiples vulnérabilités dans les produits Hitachi
- CERTA-2012-AVI-697 : Vulnérabilité dans Dovecot

- CERTA-2012-AVI-698 : Multiples vulnérabilités dans libssh
- CERTA-2012-AVI-699 : Vulnérabilité dans Google Chrome OS
- CERTA-2012-AVI-700 : Multiples vulnérabilités dans McAfee Email Gateway
- CERTA-2012-AVI-701 : Vulnérabilité dans MariaDB
- CERTA-2012-AVI-702 : Vulnérabilité dans F5 FirePass
- CERTA-2012-AVI-703 : Multiples vulnérabilités dans Xen
- CERTA-2012-AVI-704 : Multiples vulnérabilités dans Citrix XenServer

Gestion détaillée du document

07 décembre 2012 version initiale.