Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERT-FR

Paris, le 09 mars 2015
N° CERTFR-2015-ACT-010

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2015-ACT-010

1 - Recommandations relatives à l'administration sécurisée

L'ANSSI a publié le 20 février 2015 un guide proposant des recommandations pour la conception d'architectures sécurisées relatives à l'administration de systèmes d'information. Ce document revient sur les missions d'un administrateur système et les objectifs de sécurité relatifs à l'administration de ces systèmes.

Plusieurs recommandations sont proposées pour :

- la sécurisation du poste d'administration ;
- l'accès sécurisé aux ressources administrées ;
- l'utilisation sécurisée des outils d'administration est également présentée.

Le guide expose également des recommandations sur l'installation et la configuration d'annuaires et de passerelles d'administration (prenant en compte des besoins nomades). Des exemples de systèmes d'échange d'informations entre les zones admistrateur et administrées sont développés.

Enfin, le document revient sur la problématique de maintien en condition de sécurité des outils et systèmes d'administration.

Ce guide peut être consulté ou téléchargé en suivant le lien ci-dessous :
http://www.ssi.gouv.fr/uploads/2015/02/2015-02-20_NP_SDE_DAT_NT_Archi_Admin.pdf

2 - Vulnérabilités sur OpenSSL et SecureTransport (FREAK)

Une vulnérabilité affectant OpenSSL et Apple SecureTransport a été découverte par l'équipe miTLS (équipe composée de chercheurs de l'INRIA et de Microsoft).

Ces vulnérabilités affectent les versions d'OpenSSL suivantes :

- 0.9.8 jusqu'à 0.9.8zc ;
- 1.0.0 jusqu'à 1.0.0.o ;
- 1.0.1 avant 1.0.1j.

Les versions vulnérables d'OpenSSL et d'Apple SecureTransport sont utilisées dans de nombreux produits incluant le navigateur par défaut d'Android et Safari. Il est conseillé d'appliquer les mises à jour dès qu'elles seront disponibles. Dans les années 90, pour exporter de la technologie embarquant de la cryptographie en dehors des Etats-Unis, une loi obligeait les entreprises à utiliser des clés de taille faible. Pour RSA, la taille maximum autorisée était de 512 bits.

Les serveurs US devaient supporter aussi bien le chiffrement fort que le chiffrement faible, les concepteurs de SSL ont donc fait en sorte de supporter ces deux modes. Lors de la négociation, le chiffrement le plus fort supporté par le client et le serveur sera utilisé. Cette loi ayant été assouplie depuis, cette fonctionnalité est obsolète.

Toutefois, les versions d'OpenSSL citées ci-dessus acceptent toujours des clés RSA 512 bits. Il est donc possible d'effectuer une attaque de type « homme au milieu » afin de modifier la requête du client pour forcer la demande

d'une clé faible. L'attaquant pourra alors factoriser le modulo de RSA pour récupérer la clé de déchiffrement et ainsi déchiffrer le trafic SSL.

Correctif

La fonction `ssl3_get_key_exchange` permet, lors de la phase de négociation, de récupérer la clé que lui envoie le serveur. Dans les versions vulnérables, les clés d'export étaient acceptées par le client. La correction apportée pour le client consiste à refuser les clés faibles :

```
int ssl3_get_key_exchange(SSL *s){
[...]
#ifndef OPENSSL_NO_RSA
    if (alg_k & SSL_kRSA) {
        /* Temporary RSA keys only allowed in export ciphersuites */
        if (!SSL_C_IS_EXPORT(s->s3->tmp.new_cipher)) {
            al=SSL_AD_UNEXPECTED_MESSAGE;
            SSLerr(SSL_F_SSL3_GET_SERVER_CERTIFICATE,SSL_R_UNEXPECTED_MESSAGE);
            goto f_err;
        }
    [...]
}
```

Recommandations

Le CERT-FR recommande d'installer la dernière version d'OpenSSL en date qui corrige ce problème. Les mises à jour doivent également s'appliquer aux applications embarquant des versions d'OpenSSL non corrigées.

Documentation

- Entrée de blog de Matthew Green :
  http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-factoring-nsa.html
- Bulletin de sécurité OpenSSL :
  https://www.openssl.org/news/secadv_20150108.txt
- SSL FREAK Check :
  https://tools.keycdn.com/freak
- CVE-2015-0204 :
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0204
- Avis CERTFR-2015-AVI-008 du 22 décembre 2014 :
  http://www.cert.ssi.gouv.fr/site/CERTFR-2015-AVI-008/CERTFR-2015-AVI-008.html

3 - Le retour de krbtgt

Le CERT-FR a déjà présenté, dans un précédent bulletin, le compte `krbtgt` et les problématiques de sécurité associées (CERTFR-2014-ACT-032).

Pour rappel, ce compte utilisateur, présent dans tous les annuaires Active Directory et désactivé par défaut, sert de stockage aux clés des centres de distribution Kerberos.

Il est primordial que ces clés soient périodiquement renouvelées. Malheureusement, ce renouvellement n'est jamais effectué automatiquement dans les infrastructures Active Directory (à l'exception du passage d'un niveau de fonctionnalité de 2000/2003 vers 2008 ou supérieur).

Le CERT-FR a publié une procédure de changement permettant de procéder à ce renouvellement.

Le 18 février 2015, Microsoft a publié une procédure officielle de changement du mot de passe [1] pour Windows 2008 et supérieurs, associée à un script PowerShell pour simplifier la manipulation. Le CERT-FR recommande de suivre cette procédure et le script associé, afin de changer le mot de passe de tous les comptes `krbtgt` de manière périodique.

Le CERT-FR rappelle que les systèmes Windows 2000 ne sont plus supportés et peuvent, sous certaines conditions, entraîner des problèmes d'authentification (CERTFR-2014-ACT-047). De plus, ces systèmes n'ont pas bénéficié du correctif MS14-068 et peuvent être très facilement compromis (CERTFR-2014-ALE-011).

Concernant les systèmes Windows 2003, le CERT-FR rappelle que la fin du support est programmée au 14 juillet 2015, soit dans 4 mois. Il convient donc de procéder dans les plus brefs délais à leur migration.

Documentation

- Bulletin de Microsoft [1] :
  http://blogs.microsoft.com/cybertrust/2015/02/11/krbtgt-account-password-reset-scripts
- Bulletin d'actualité CERTFR-2014-ACT-032 :
  http://www.cert.ssi.gouv.fr/site/CERTFR-2014-ACT-032/
- Alerte CERTFR-2014-ALE-011 :
  http://www.cert.ssi.gouv.fr/site/CERTFR-2014-ALE-011

4 - Rappel des avis émis

Dans la période du 02 au 08 mars 2015, le CERT-FR a émis les publications suivantes :

- CERTFR-2015-AVI-082 : Vulnérabilité dans le noyau Linux
- CERTFR-2015-AVI-083 : Vulnérabilité dans le pilote Nvidia
- CERTFR-2015-AVI-084 : Multiples vulnérabilités dans les produits Avaya
- CERTFR-2015-AVI-085 : Multiples vulnérabilités dans le noyau Linux de Redhat
- CERTFR-2015-AVI-086 : Multiples vulnérabilités dans Google Chrome
- CERTFR-2015-AVI-087 : Multiples vulnérabilités dans Wireshark
- CERTFR-2015-AVI-088 : Multiples vulnérabilités dans Xen
- CERTFR-2015-AVI-089 : Multiples vulnérabilités dans OpenSSL

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

- CERTFR-2015-AVI-081 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu (mise à jour suite à la correction d'une régression.)

Gestion détaillée du document

09 mars 2015 version initiale.