Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 18 mai 2000
N° CERTA-2000-AVI-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Débordements de variables dans les services authentifiés par Kerberos

Gestion du document

Date de la première version	18 mai 2000
Date de la dernière version	–
Source(s)	Avis CA-2000-06 du CERT/CC Avis de l'équipe Kerberos du MIT

TAB. 1 – *gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 Systèmes concernés

- les systèmes faisant fonctionner des services authentifiés par Kerberos 4 ;
- certains systèmes faisant fonctionner des services authentifiés par Kerberos 5 ;
- les systèmes faisant fonctionner le démon de shell distant « kerbérisé » (*krshd*) ;
- les systèmes sur lesquels l'utilitaire *ksu* de kerberos 5 est installé ;
- les systèmes sur lesquels l'utilitaire *krcp* de kerberos 5 est installé ;

2 Résumé

Le *CERT Coordination Center* a récemment été informé de plusieurs vulnérabilités liées à des débordements de variables dans leur logiciel d'authentification Kerberos. La vulnérabilité la plus grave permet à des intrus distants d'obtenir les privilèges de *root* sur le système sur lequel tourne les services qui utilisent l'authentification de Kerberos. Si des services vulnérables sont autorisés sur le système servant de Centre de Distribution des clefs (KDC), il se peut que le domaine Kerberos entier soit compromis.

3 Risque

Les logiciels vulnérables peuvent permettre à des intrus d'obtenir l'accès aux privilèges de *root*.
Le risque est réel puisque des exploitations de ces vulnérabilités ont été publiées.

4 Description

Il y a au moins quatre vulnérabilités distinctes dans les différentes versions et implémentations du logiciel Kerberos. Toutes ces vulnérabilités peuvent être exploitées pour obtenir les privilèges de *root*.

Débordement de variable dans la fonction `krb_rd_req()` Cette vulnérabilité est présente dans la version 4 de Kerberos. Elle est aussi présente dans la version 5 (dans le mode de compatibilité avec la version 4). Cette vulnérabilité peut être exploitée dans les services qui utilisent la version 4 ou la version 5 quand ils effectuent de l'authentification selon la version 4. Cette vulnérabilité peut aussi être exploitée localement à travers le programme de Kerberos 5 *v4rcp* qui est *setuid root*.
Il se peut que cette vulnérabilité soit exploitable dans la version 4. Cette vulnérabilité est exploitable dans la version (en conjonction avec la vulnérabilité de la fonction `krb425_conv_principal()`, décrite plus loin).

Débordement de variable dans la fonction `krb425_conv_principal()` Cette vulnérabilité est présente dans le code de compatibilité ascendante de la version 5. Cette vulnérabilité est connue pour être exploitable dans la version 5 en conjonction avec une exploitation de la vulnérabilité concernant `krb_rd_req()`.

Débordement de variables dans `krshd` Cette vulnérabilité est seulement présente dans la version 5. Cette vulnérabilité n'est pas liée aux autres vulnérabilités.

Débordement de variable dans `ksu` Cette vulnérabilité est seulement présente dans la version 5 et est corrigée dans les versions *krb5-1.1.1* et *krb5-1.0.7-beta1*. La vulnérabilité de *ksu* n'est pas liée aux autres vulnérabilités.

5 Contournement provisoire

Provisoirement par des configuration il est possible de se prémunir contre certaines vulnérabilités :

- certains *daemons* lancés par *inetd* peuvent s'avérer plus sûr contre l'exploitation de la vulnérabilité si la ligne de commande qui les invoque est modifiée pour exclure l'usage de Kerberos 4 pour l'authentification. Consultez la page de manuel de votre distribution Kerberos pour déterminer la ligne de commande correcte pour désactiver l'authentification Kerberos 4. Les *daemons* pour lesquels il se peut qu'une telle démarche fonctionne incluent :
  - *krshd*[1] ;
  - klogind ;
  - telnetd.
- les permissions *setuid* du programme *v4rcp* doivent être retirées pour éviter une exploitation locale de la vulnérabilité ;
- les permissions *setuid* du programme du programme *krb5 ksu* doivent être retirées s'il n'a pas été compilé depuis les distributions *krb5-1.1.1*, *krb5-1.0.7-beta1* ou ultérieures. Il semble sûr de remplacer l'exécutable *ksu* par un nouvel exécutable compilé à partir des distributions *krb5-1.1.1* ou *krb5-1.0.7-beta1* pourvu qu'il ne soit pas compilé avec des bibliothèques partagées (la vulnéravilité est due à certains bogues dans les bibliothèques). Si *ksu* a été compilé avec des bibliothèques partagées, il vaut mieux installer une nouvelle version pour laquelle le bogue dans la bibliothèque a été résolu.
- dans la distribution du MIT de Kerberos 5, il se peut qu'il ne soit pas possible de désactiver l'authentification Kerberos 4 dans le programme *ftpd*. Notez que seules les versions *krb5-1.1.1* et ultérieures ont la capacité de recevoir des authentification Kerberos 4.

6 Solution

6.1 Appliquez le patch de votre fournisseur

Si votre fournisseur n'apparaît pas dans la liste, veuillez contacter le CERTA.

1. *krshd* restera néanmoins vulnérable à une attaque distante même si l'authentification Kerberos 4 est désactivée, en raison de l'autre débordement de variable évoqué plus bas. Il vaut mieux désactiver le daemon *krshd* complètement jusqu'à ce qu'une version de patch soit disponible.

6.1.1 Microsoft

Aucun produit Microsoft n'est touché par cette vulnérabilité.

6.1.2 MIT Kerberos

L'avis du MIT sur ce sujet est disponible sur :
http://web.mit.edu/kerberos/www/advisories/krb4buf.txt

6.1.3 NetBSD

NetBSD possède deux référentiels de codes pour les logiciels cryptographiques en raison des lois américaines concernant l'export (et aussi des considérations ayant trait à des brevets).

L'arborescence *crypto-intl* destiné à l'utilisation hors des États-Unis n'est pas affecté.

6.1.4 OpenBSD

OpenBSD utilise la ditribution KTH de Kerberos, qui est réputée non vulnérable.

6.1.5 L'université de Washington

Les logiciels publiés par l'Université de Washington ne sont pas distribués sous forme de distribution binaire. C'est à l'installateur de décider à la compilation si il utilise ou non Kerberos.

Les serveurs POP3 et IMAP de l'Université de Washington sont basés sur Kerberos 5 et ne font jamais appel à Kerberos 4. A ce titre il ne sont pas vulnérables.

6.1.6 Autres

La meilleure action à conseiller est de patcher le code dans la bibliothèque *krb4* et en outre patcher le code du programme *krshd*. Les patches suivants incluent des corrections moins essentielles qui affectent aussi les débordement de variable dans du code potentiellement vulnérable, mais pour lesquels l'exploitation des vulnérabilités est sensiblement plus difficile à construire.

Les patches sont disponibles à l'URL
http://www.cert.org/advisories/CA-2000-06/mit_10x_patch.txt

Gestion détaillée du document

18 mai 2000 version initiale.