

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités sur le serveur FTP utilisant Kerberos 5

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-2000-AVI-007>

Gestion du document

Référence	CERTA-2000-AVI-007
Titre	Vulnérabilités sur le serveur FTP utilisant Kerberos 5
Date de la première version	15 juin 2000
Date de la dernière version	–
Source(s)	CERT IST Masachuset's Institute of Technology (MIT)

TAB. 1 – gestion du document

1 Risques

- Accès root
- Déni de service
- Execution de commandes non-autorisées

2 Systèmes concernés

Kerberos 5 releases krb5-1.1 et krb5-1.1.1, ainsi que les version beta krb5-1.1.2-beta1 krb5-1.2-beta2

3 Description

GSSFTP est un serveur FTP sécurisé utilisant la suite Kerberos 5 du MIT. Deux vulnérabilités y ont été découvertes :

- Un utilisateur ayant un accès local au serveur FTP peut obtenir les privilèges de root lui permettant d'exécuter des commandes qui ne lui sont pas autorisées.
- Un utilisateur distant peut effectuer un déni de service.

Windows 2000 repose sur les mécanismes d'authentification offerts par le protocole Kerberos 5. À ce titre, un client ftp sous Windows peut s'authentifier auprès d'un serveur GSSFTP compromis donnant ainsi un faux sentiment de sécurité.

4 Solutions

1° Appliquer le correctif concernant la vulnérabilité de GSSFTP pour les releases krb5-1.1 et krb.5-1.1.1 de kerberos 5 se trouvant à l'adresse suivante :

http://web.mit.edu/kerberos/www/advisories/ftpd_111_patch.txt

2° Mettre à jour la version 1.2 de Kerberos 5 (voir l'adresse qui suit) :

<http://web.mit.edu/kerberos/www>

5 Documentation

Avis de sécurité du MIT :

<http://web.mit.edu/kerberos/www/advisories/ftp.txt>