Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 30 avril 2004
N° CERTA-2004-AVI-088-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du serveur SAMBA

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-2004-AVI-088

Gestion du document

Référence	CERTA-2004-AVI-088-002
Titre	Vulnérabilité du serveur SAMBA
Date de la première version	15 mars 2004
Date de la dernière version	30 avril 2004
Source(s)	Avis de sécurité ISS
Pièce(s) jointe(s)	Aucune

TAB. 1 – *gestion du document*

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

1 Risque

- Elévation de privilèges d'un utilisateur local ;
- contournement de la politique de sécurité.

2 Systèmes affectés

Tout système *Unix* utilisant *Samba* en mode client.

3 Résumé

Une mauvaise gestion des privilèges associés à l'utilitaire *smbmnt* permet à un utilisateur mal intentionné d'utiliser localement des programmes avec des droits arbitraires.

4 Description

Samba met en oeuvre les protocoles Microsoft de partage de fichiers et imprimantes SMB/CIFS ("Server Message Block/Common Internet File System").

L'utilitaire *smbmnt* permet à une station client de monter localement un système de fichier distant depuis un serveur Samba. Pour permettre son emploi par un utilisateur quelconque, cette commande est souvent installée avec une délégation des privilèges de l'administrateur (*suid root*). Il est alors possible d'exécuter localement les programmes situés dans l'arborescence montée, mais avec les délégations de privilèges configurées dans le système distant. Si le serveur Samba peut être arbitrairement choisi, l'utilisateur local disposant d'un serveur sous son contrôle obtient alors tous les privilèges.

5 Contournement provisoire

Supprimer la délégation de privilèges pour *smbmnt*.

6 Solution

Mettre à jour en fonction des recommandations du distributeur.

- Bulletin de sécurité Debian GNU/linux DSA-463 :
  http://www.debian.org/security/2004/dsa-463.fr.html
- Bulletin de sécurité Mandrake MDKSA-2004:035 :
  http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2004:035
- Bulletin de sécurité Gentoo GLSA 200404-21 :
  http://www.gentoo.org/security/en/glsa/glsa-200404-21.xml

7 Documentation

- Avis de sécurité ISS X-Force :
  http://xforce.iss.net/xforce/xfdb/15131
- Note de vulnérabilité SecurityFocus :
  http://www.securityfocus.com/bid/9619/info/
- Référence CVE CAN-2004-0186 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0186

Gestion détaillée du document

15 mars 2004 version initiale.
20 avril 2004 ajout de la référence au bulletin de sécurité Mandrake.
30 avril 2004 ajout de la référence au bulletin de sécurité Gentoo.