

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : vulnérabilités de RPC.statd sous Linux

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-039>

Gestion du document

Référence	CERTA-2000-AVI-39
Titre	vulnérabilités de RPC.statd sous Unix
Date de la première version	30 août 2000
Date de la dernière version	–
Source(s)	Avis CA-2000-17 du CERT/CC Avis du CIAC
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

Accès root à distance sans compte utilisateur

2 Systèmes affectés

Systèmes Unix et Linux possédant RPC.statd.

3 Résumé

Le daemon RPC.statd intervient dans le fonctionnement du service NFS sous Unix. Ce daemon possède une vulnérabilité permettant à un utilisateur distant d'exécuter du code ou d'accéder à un shell avec les privilèges root. Les exploits utilisant les vulnérabilités de RPC.statd se multiplient toujours.

4 Description

Le Daemon RPC.statd passe des informations fournies par les utilisateur du service à la fonction syslog() (journalisation) et manipule des fichiers avec les privilèges de root par défaut. Un défaut dans la conception de ce daemon permet à un utilisateur mal intentionné d'injecter dans les données transmises à syslog du code exécutable avec les privilèges de RPC.statd (typiquement ceux de root).

5 Contournement provisoire

Désactiver RPC.statd ou NFS s'il n'est pas utile au fonctionnement du système et des réseaux.

6 Solution

Mettre à jour RPC.statd selon le système que vous avez :

- Connectiva Linux 5.1:
<ftp://ftp.conectiva.com.br/pub/conectiva/atualizacoes/5.1/i386/nfs-utils-0.1.9.1-4cl.i386.rpm>
- Connectiva Linux 5.0:
<ftp://ftp.conectiva.com.br/pub/conectiva/atualizacoes/5.0/i386/nfs-utils-0.1.9.1-3cl.i386.rpm>
- Connectiva Linux 4.2:
<ftp://ftp.conectiva.com.br/pub/conectiva/atualizacoes/4.2/i386/nfs-utils-0.1.9.1-3cl.i386.rpm>
- Connectiva Linux 4.1:
<ftp://ftp.conectiva.com.br/pub/conectiva/atualizacoes/4.1/i386/nfs-utils-0.1.9.1-3cl.i386.rpm>
- Connectiva Linux 4.0es:
<ftp://ftp.conectiva.com.br/pub/conectiva/atualizacoes/4.0es/i386/nfs-utils-0.1.9.1-3cl.i386.rpm>
- Connectiva Linux 4.0:
<ftp://ftp.conectiva.com.br/pub/conectiva/atualizacoes/4.0/i386/nfs-utils-0.1.9.1-3cl.i386.rpm>
- Debian Linux pour powerpc:
http://http.us.debian.org/debian/dists/unstable/main/binary-powerpc/net/nfs-common_0.1.9.1-1.deb
- Debian Linux pour PC:
http://http.us.debian.org/debian/dists/unstable/main/binary-i386/net/nfs-common_0.1.9.1-1.deb
- Debian Linux pour sparc:
http://http.us.debian.org/debian/dists/unstable/main/binary-sparc/net/nfs-common_0.1.9.1-1.deb
- Debian Linux pour alpha:
http://http.us.debian.org/debian/dists/potato/main/binary-alpha/net/nfs-common_0.1.9.1-1.deb
- RedHat Linux pour sparc:
<ftp://updates.redhat.com/6.2/sparc/nfs-utils-0.1.9.1-1.sparc.rpm>
- RedHat Linux i386:
<ftp://updates.redhat.com/6.2/i386/nfs-utils-0.1.9.1-1.i386.rpm>
- RedHat Linux alpha:
<ftp://updates.redhat.com/6.2/alpha/nfs-utils-0.1.9.1-1.alpha.rpm>
- Trustix Trustix Secure Linux
<ftp://ftp.trustix.com/pub/Trustix/updates/1.1/RPMS/nfs-utils-0.1.9.1-1tr.i586.rpm>
- Suse Linux selon la version :
<ftp://ftp.suse.com/pub/suse/i386/update/6.4/nl/knfsd.rpm>
<ftp://ftp.suse.com/pub/suse/i386/update/6.4/zql/knfsd.rpm>
<ftp://ftp.suse.com/pub/suse/i386/update/6.3/nl/knfsd.rpm>
<ftp://ftp.suse.com/pub/suse/i386/update/6.3/zql/knfsd.rpm>
<ftp://ftp.suse.com/pub/suse/i386/update/6.2/nl/linuxnfs.rpm>
<ftp://ftp.suse.com/pub/suse/i386/update/6.2/zql/linuxnfs.rpm>
<ftp://ftp.suse.com/pub/suse/i386/update/6.1/nl/linuxnfs.rpm>
<ftp://ftp.suse.com/pub/suse/i386/update/6.1/zql/linuxnfs.rpm>
<ftp://ftp.suse.com/pub/suse/axp/update/6.4/nl/knfsd.rpm>
<ftp://ftp.suse.com/pub/suse/axp/update/6.4/zql/knfsd.rpm>

ftp://ftp.suse.com/pub/suse/axp/update/6.3/nl/knfsd.rpm
ftp://ftp.suse.com/pub/suse/axp/update/6.3/zql/knfsd.rpm
ftp://ftp.suse.com/pub/suse/axp/update/6.1/nl/linuxnfs.rpm
ftp://ftp.suse.com/pub/suse/axp/update/6.1/zql/linuxnfs.rpm
ftp://ftp.suse.com/pub/suse/ppc/update/6.4/nl/knfsd.rpm
ftp://ftp.suse.com/pub/suse/ppc/update/6.4/zql/knfsd.rpm

Nota : Cette liste n'est pas exhaustive car elle s'agrandit de jour en jour. Il existe, depuis longtemps, de nombreuses vulnérabilités liées RPC.statd pour SunOS et solaris. Pour savoir s'il existe une mise à jour de RPC.statd pour votre système, contactez votre éditeur.

7 Documentation

- Avis du CERT/CC
<http://www.cert.org/advisories/CA-2000-17.html>
- Avis du CIAC :
<http://www.ciac.org/ciac/bulletins/k-069.shtml>

Gestion détaillée du document

30 août 2000 version initiale.