

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité dans la bibliothèque glibc sous Unix

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-ALE-014>

Gestion du document

Référence	CERTA-2000-ALE-014
Titre	Vulnérabilité dans la bibliothèque glibc sous Unix
Date de la première version	14 septembre 2000
Date de la dernière version	–
Source(s)	Avis de sécurité Debian et RedHat Avis Security Bugware
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 en local grâce à un débordement de pile.

2 Systèmes affectés

Systèmes Unix basés sur la glibc.

3 Résumé

La bibliothèque glibc permet à un utilisateur local d'exécuter du code arbitraire avec les privilèges de root.

4 Description

Un utilisateur mal intentionné peut, à l'aide de débordements de piles dans les programmes ayant le bit `suid` activé, obtenir des droits qu'il n'a pas (en général `root`), en faisant appel à une faille dans la bibliothèque glibc.

Ces programmes sont entre autres :

- /bin/su
- /bin/mount
- /bin/umount
- /usr/bin/
- /usr/bin/lpq
- /usr/bin/passwd
- /usr/bin/at
- /usr/bin/suidperl
- /usr/sbin/usernetcl
- /usr/sbin/userhelper

Ces utilitaires sont pour la plupart nécessaires au fonctionnement du système.

5 Solution

Appliquer les correctifs obtenus par les adresses suivantes :

- Debian :
 - http://security.debian.org/dists/stable/updates/main/source/glibc_2.1.3-13.diff.gz
 - http://security.debian.org/dists/stable/updates/main/source/glibc_2.1.3-13.dsc
 - http://security.debian.org/dists/stable/updates/main/source/glibc_2.1.3.orig.tar.gz
 - http://security.debian.org/dists/stable/updates/main/binary-all/glibc-doc_2.1.3-13_all.deb
 - http://security.debian.org/dists/stable/updates/main/binary-all/i18ndata_2.1.3-13_all.deb
 - http://security.debian.org/dists/stable/updates/main/binary-alpha/libc6.1-dbg_2.1.3-13_alpha.deb
 - http://security.debian.org/dists/stable/updates/main/binary-alpha/libc6.1-dev_2.1.3-13_alpha.deb
 - http://security.debian.org/dists/stable/updates/main/binary-alpha/libc6.1-pic_2.1.3-13_alpha.deb
 - http://security.debian.org/dists/stable/updates/main/binary-alpha/libc6.1-prof_2.1.3-13_alpha.deb
 - http://security.debian.org/dists/stable/updates/main/binary-alpha/libc6.1_2.1.3-13_alpha.deb
 - http://security.debian.org/dists/stable/updates/main/binary-alpha/libnss1-compat_2.1.3-13_alpha.deb
 - http://security.debian.org/dists/stable/updates/main/binary-alpha/locales_2.1.3-13_alpha.deb
 - http://security.debian.org/dists/stable/updates/main/binary-alpha/nscd_2.1.3-13_alpha.deb
 - http://security.debian.org/dists/stable/updates/main/binary-arm/libc6-dbg_2.1.3-13_arm.deb
 - http://security.debian.org/dists/stable/updates/main/binary-arm/libc6-dev_2.1.3-13_arm.deb
 - http://security.debian.org/dists/stable/updates/main/binary-arm/libc6-pic_2.1.3-13_arm.deb
 - http://security.debian.org/dists/stable/updates/main/binary-arm/libc6-prof_2.1.3-13_arm.deb
 - http://security.debian.org/dists/stable/updates/main/binary-arm/libc6_2.1.3-13_arm.deb
 - http://security.debian.org/dists/stable/updates/main/binary-arm/locales_2.1.3-13_arm.deb
 - http://security.debian.org/dists/stable/updates/main/binary-arm/nscd_2.1.3-13_arm.deb
 - http://security.debian.org/dists/stable/updates/main/binary-i386/libc6-dbg_2.1.3-13_i386.deb
 - http://security.debian.org/dists/stable/updates/main/binary-i386/libc6-dev_2.1.3-13_i386.deb
 - http://security.debian.org/dists/stable/updates/main/binary-i386/libc6-pic_2.1.3-13_i386.deb
 - http://security.debian.org/dists/stable/updates/main/binary-i386/libc6-prof_2.1.3-13_i386.deb
 - http://security.debian.org/dists/stable/updates/main/binary-i386/libc6_2.1.3-13_i386.deb
 - http://security.debian.org/dists/stable/updates/main/binary-i386/libnss1-compat_2.1.3-13_i386.deb
 - http://security.debian.org/dists/stable/updates/main/binary-i386/locales_2.1.3-13_i386.deb
 - http://security.debian.org/dists/stable/updates/main/binary-i386/nscd_2.1.3-13_i386.deb
 - http://security.debian.org/dists/stable/updates/main/binary-powerpc/libc6-dbg_2.1.3-13_powerpc.deb
 - http://security.debian.org/dists/stable/updates/main/binary-powerpc/libc6-dbg_2.1.3-13_powerpc.deb
 - http://security.debian.org/dists/stable/updates/main/binary-powerpc/libc6-pic_2.1.3-13_powerpc.deb
 - http://security.debian.org/dists/stable/updates/main/binary-powerpc/libc6-prof_2.1.3-13_powerpc.deb

- http://security.debian.org/dists/stable/updates/main/binary-powerpc/libc6_2.1.3-13_powerpc.deb
 - http://security.debian.org/dists/stable/updates/main/binary-powerpc/locales_2.1.3-13_powerpc.deb
 - http://security.debian.org/dists/stable/updates/main/binary-powerpc/nscd_2.1.3-13_powerpc.deb
 - http://security.debian.org/dists/stable/updates/main/binary-sparc/libc6-dbg_2.1.3-13_sparc.deb
 - http://security.debian.org/dists/stable/updates/main/binary-sparc/libc6-dev_2.1.3-13_sparc.deb
 - http://security.debian.org/dists/stable/updates/main/binary-sparc/libc6-pic_2.1.3-13_sparc.deb
 - http://security.debian.org/dists/stable/updates/main/binary-sparc/libc6-prof_2.1.3-13_sparc.deb
 - http://security.debian.org/dists/stable/updates/main/binary-sparc/libc6_2.1.3-13_sparc.deb
 - http://security.debian.org/dists/stable/updates/main/binary-sparc/locales_2.1.3-13_sparc.deb
 - http://security.debian.org/dists/stable/updates/main/binary-sparc/nscd_2.1.3-13_sparc.deb
 - http://security.debian.org/dists/slink/updates/source/glibc_2.0.7.19981211-6.3.diff.gz
 - http://security.debian.org/dists/slink/updates/source/glibc_2.0.7.19981211-6.3.dsc
 - http://security.debian.org/dists/slink/updates/source/glibc_2.0.7.19981211.orig.tar.gz
 - http://security.debian.org/dists/slink/updates/binary-i386/libc6-dbg_2.0.7.19981211-6.3_i386.deb
 - http://security.debian.org/dists/slink/updates/binary-i386/libc6-dev_2.0.7.19981211-6.3_i386.deb
 - http://security.debian.org/dists/slink/updates/binary-i386/libc6-pic_2.0.7.19981211-6.3_i386.deb
 - http://security.debian.org/dists/slink/updates/binary-i386/libc6_2.0.7.19981211-6.3_i386.deb
 - http://security.debian.org/dists/slink/updates/binary-i386/locales_2.0.7.19981211-6.3_i386.deb
 - http://security.debian.org/dists/slink/updates/binary-i386/timezones_2.0.7.19981211-6.3_i386.deb
- Conectiva :
- <ftp://atualizacoes.conectiva.com.br/4.0/SRPMS/glibc-2.1.2-14cl.src.rpm>
 - <ftp://atualizacoes.conectiva.com.br/4.0/i386/glibc-2.1.2-14cl.i386.rpm>
 - <ftp://atualizacoes.conectiva.com.br/4.0/i386/glibc-devel-2.1.2-14cl.i386.rpm>
 - <ftp://atualizacoes.conectiva.com.br/4.0/i386/glibc-profile-2.1.2-14cl.i386.rpm>
 - <ftp://atualizacoes.conectiva.com.br/4.0/i386/nscd-2.1.2-14cl.i386.rpm>
 - <ftp://atualizacoes.conectiva.com.br/4.0es/SRPMS/glibc-2.1.2-14cl.src.rpm>
 - <ftp://atualizacoes.conectiva.com.br/4.0es/i386/glibc-2.1.2-14cl.i386.rpm>
 - <ftp://atualizacoes.conectiva.com.br/4.0es/i386/glibc-devel-2.1.2-14cl.i386.rpm>
 - <ftp://atualizacoes.conectiva.com.br/4.0es/i386/glibc-profile-2.1.2-14cl.i386.rpm>
 - <ftp://atualizacoes.conectiva.com.br/4.0es/i386/nscd-2.1.2-14cl.i386.rpm>
 - <ftp://atualizacoes.conectiva.com.br/4.1/SRPMS/glibc-2.1.2-14cl.src.rpm>
 - <ftp://atualizacoes.conectiva.com.br/4.1/i386/glibc-2.1.2-14cl.i386.rpm>
 - <ftp://atualizacoes.conectiva.com.br/4.1/i386/glibc-devel-2.1.2-14cl.i386.rpm>
 - <ftp://atualizacoes.conectiva.com.br/4.1/i386/glibc-profile-2.1.2-14cl.i386.rpm>
 - <ftp://atualizacoes.conectiva.com.br/4.1/i386/nscd-2.1.2-14cl.i386.rpm>
 - <ftp://atualizacoes.conectiva.com.br/4.2/SRPMS/glibc-2.1.2-14cl.src.rpm>
 - <ftp://atualizacoes.conectiva.com.br/4.2/i386/glibc-2.1.2-14cl.i386.rpm>
 - <ftp://atualizacoes.conectiva.com.br/4.2/i386/glibc-devel-2.1.2-14cl.i386.rpm>
 - <ftp://atualizacoes.conectiva.com.br/4.2/i386/glibc-profile-2.1.2-14cl.i386.rpm>
 - <ftp://atualizacoes.conectiva.com.br/4.2/i386/nscd-2.1.2-14cl.i386.rpm>
 - <ftp://atualizacoes.conectiva.com.br/5.0/SRPMS/glibc-2.1.3-10cl.src.rpm>
 - <ftp://atualizacoes.conectiva.com.br/5.0/i386/glibc-2.1.3-10cl.i386.rpm>
 - <ftp://atualizacoes.conectiva.com.br/5.0/i386/glibc-devel-2.1.3-10cl.i386.rpm>
 - <ftp://atualizacoes.conectiva.com.br/5.0/i386/glibc-profile-2.1.3-10cl.i386.rpm>
 - <ftp://atualizacoes.conectiva.com.br/5.0/i386/nscd-2.1.3-10cl.i386.rpm>
 - <ftp://atualizacoes.conectiva.com.br/5.1/SRPMS/glibc-2.1.3-10cl.src.rpm>
 - <ftp://atualizacoes.conectiva.com.br/5.1/i386/glibc-2.1.3-10cl.i386.rpm>
 - <ftp://atualizacoes.conectiva.com.br/5.1/i386/glibc-devel-2.1.3-10cl.i386.rpm>
 - <ftp://atualizacoes.conectiva.com.br/5.1/i386/glibc-profile-2.1.3-10cl.i386.rpm>
 - <ftp://atualizacoes.conectiva.com.br/5.1/i386/nscd-2.1.3-10cl.i386.rpm>

- <ftp://atualizacoes.conectiva.com.br/ferramentas/ecommerce/SRPMS/glibc-2.1.3-10cl.src.rpm>
 - <ftp://atualizacoes.conectiva.com.br/ferramentas/ecommerce/i386/glibc-2.1.3-10cl.i386.rpm>
 - <ftp://atualizacoes.conectiva.com.br/ferramentas/ecommerce/i386/glibc-devel-2.1.3-10cl.i386.rpm>
 - <ftp://atualizacoes.conectiva.com.br/ferramentas/ecommerce/i386/glibc-profile-2.1.3-10cl.i386.rpm>
 - <ftp://atualizacoes.conectiva.com.br/ferramentas/ecommerce/i386/nscd-2.1.3-10cl.i386.rpm>
 - <ftp://atualizacoes.conectiva.com.br/ferramentas/graficas/SRPMS/glibc-2.1.3-10cl.src.rpm>
 - <ftp://atualizacoes.conectiva.com.br/ferramentas/graficas/i386/glibc-2.1.3-10cl.i386.rpm>
 - <ftp://atualizacoes.conectiva.com.br/ferramentas/graficas/i386/glibc-devel-2.1.3-10cl.i386.rpm>
 - <ftp://atualizacoes.conectiva.com.br/ferramentas/graficas/i386/glibc-profile-2.1.3-10cl.i386.rpm>
 - <ftp://atualizacoes.conectiva.com.br/ferramentas/graficas/i386/nscd-2.1.3-10cl.i386.rpm>
- Caldera :
- OpenLinux Desktop 2.3 :
 - <ftp://ftp.calderasystems.com/pub/updates/OpenLinux/2.3/current/RPMS/>
 - <ftp://ftp.calderasystems.com/pub/updates/OpenLinux/2.3/current/SRPMS/>
 - [RPMS/glibc-2.1.1-3.i386.rpm](#)
 - [RPMS/glibc-devel-2.1.1-3.i386.rpm](#)
 - [RPMS/glibc-devel-static-2.1.1-3.i386.rpm](#)
 - [RPMS/glibc-localedata-2.1.1-3.i386.rpm](#)
 - [SRPMS/glibc-2.1.1-3.src.rpm](#)
 - OpenLinux eServer 2.3 et OpenLinux eBuilder pour ECential 3.0 :
 - <ftp://ftp.calderasystems.com/pub/updates/eServer/2.3/current/RPMS/>
 - <ftp://ftp.calderasystems.com/pub/updates/eServer/2.3/current/SRPMS/>
 - [RPMS/glibc-2.1.3-4S.i386.rpm](#)
 - [RPMS/glibc-devel-2.1.3-4S.i386.rpm](#)
 - [RPMS/glibc-devel-static-2.1.3-4S.i386.rpm](#)
 - [RPMS/glibc-localedata-2.1.3-4S.i386.rpm](#)
 - [SRPMS/glibc-2.1.3-4S.src.rpm](#)
 - OpenLinux eDesktop 2.4 :
 - <ftp://ftp.calderasystems.com/pub/updates/eDesktop/2.4/current/RPMS/>
 - <ftp://ftp.calderasystems.com/pub/updates/eDesktop/2.4/current/SRPMS/>
 - [RPMS/glibc-2.1.2-7.i386.rpm](#)
 - [RPMS/glibc-devel-2.1.2-7.i386.rpm](#)
 - [RPMS/glibc-devel-static-2.1.2-7.i386.rpm](#)
 - [RPMS/glibc-localedata-2.1.2-7.i386.rpm](#)
 - [SRPMS/glibc-2.1.2-7.src.rpm](#)
- Slackware:
- <ftp://ftp.slackware.com/pub/slackware/slackware-current/slakware/a1/glibcso.tgz>
 - <ftp://ftp.slackware.com/pub/slackware/slackware-current/slakware/d1/glibc.tgz>
 - <ftp://ftp.slackware.com/pub/slackware/slackware-current/slakware/des1/descript.tgz>
- SuSE Linux:
- <ftp://ftp.suse.com/pub/suse/i386/update/7.0/a1/shlibs-2.1.3-154.i386.rpm>
 - <ftp://ftp.suse.com/pub/suse/i386/update/7.0/d1/libc-2.1.3-154.i386.rpm>
 - <ftp://ftp.suse.com/pub/suse/i386/update/7.0/d2/libd-2.1.3-154.i386.rpm>
 - <ftp://ftp.suse.com/pub/suse/i386/update/7.0/zq1/libc-2.1.3-154.src.rpm>
 - <ftp://ftp.suse.com/pub/suse/i386/update/6.4/a1/shlibs-2.1.3-154.i386.rpm>

- ftp://ftp.suse.com/pub/suse/i386/update/6.4/d1/libc-2.1.3-154.i386.rpm
 - ftp://ftp.suse.com/pub/suse/i386/update/6.4/d2/libd-2.1.3-154.i386.rpm
 - ftp://ftp.suse.com/pub/suse/i386/update/6.4/zq1/libc-2.1.3-154.src.rpm
 - ftp://ftp.suse.com/pub/suse/i386/update/6.3/a1/shlibs-2.1.2-47.i386.rpm
 - ftp://ftp.suse.com/pub/suse/i386/update/6.3/d1/libc-2.1.2-47.i386.rpm
 - ftp://ftp.suse.com/pub/suse/i386/update/6.3/d2/libd-2.1.2-47.i386.rpm
 - ftp://ftp.suse.com/pub/suse/i386/update/6.3/zq1/libc-2.1.2-47.src.rpm
 - ftp://ftp.suse.com/pub/suse/i386/update/6.2/a1/shlibs-2.1.1-29.i386.rpm
 - ftp://ftp.suse.com/pub/suse/i386/update/6.2/d1/libc-2.1.1-29.i386.rpm
 - ftp://ftp.suse.com/pub/suse/i386/update/6.2/d2/libd-2.1.1-29.i386.rpm
 - ftp://ftp.suse.com/pub/suse/i386/update/6.2/zq1/libc-2.1.1-29.src.rpm
 - ftp://ftp.suse.com/pub/suse/i386/update/6.1/a1/shlibs-2000.9.5-0.i386.rpm
 - ftp://ftp.suse.com/pub/suse/i386/update/6.1/d1/libc-2000.9.5-0.i386.rpm
 - ftp://ftp.suse.com/pub/suse/i386/update/6.1/d2/libd-2000.9.5-0.i386.rpm
 - ftp://ftp.suse.com/pub/suse/i386/update/6.1/zq1/libc-2000.9.5-0.src.rpm
 - ftp://ftp.suse.com/pub/suse/sparc/update/7.0/a1/shlibs-2.1.3-154.sparc.rpm
 - ftp://ftp.suse.com/pub/suse/sparc/update/7.0/d1/libc-2.1.3-154.sparc.rpm
 - ftp://ftp.suse.com/pub/suse/sparc/update/7.0/d2/libd-2.1.3-154.sparc.rpm
 - ftp://ftp.suse.com/pub/suse/sparc/update/7.0/zq1/libc-2.1.3-154.src.rpm
 - ftp://ftp.suse.com/pub/suse/axp/update/6.4/a1/shlibs-2.1.3-154.alpha.rpm
 - ftp://ftp.suse.com/pub/suse/axp/update/6.4/d1/libc-2.1.3-154.alpha.rpm
 - ftp://ftp.suse.com/pub/suse/axp/update/6.4/d2/libd-2.1.3-154.alpha.rpm
 - ftp://ftp.suse.com/pub/suse/axp/update/6.4/zq1/libc-2.1.3-154.src.rpm
 - ftp://ftp.suse.com/pub/suse/axp/update/6.3/a1/shlibs-2.1.2-47.alpha.rpm
 - ftp://ftp.suse.com/pub/suse/axp/update/6.3/d1/libc-2.1.2-47.alpha.rpm
 - ftp://ftp.suse.com/pub/suse/axp/update/6.3/d2/libd-2.1.2-47.alpha.rpm
 - ftp://ftp.suse.com/pub/suse/axp/update/6.3/zq1/libc-2.1.2-47.src.rpm
 - ftp://ftp.suse.com/pub/suse/axp/update/6.1/a1/shlibs-2000.9.5-0.alpha.rpm
 - ftp://ftp.suse.com/pub/suse/axp/update/6.1/d1/libc-2000.9.5-0.alpha.rpm
 - ftp://ftp.suse.com/pub/suse/axp/update/6.1/d2/libd-2000.9.5-0.alpha.rpm
 - ftp://ftp.suse.com/pub/suse/axp/update/6.1/zq1/libc-2000.9.5-0.src.rpm
 - ftp://ftp.suse.com/pub/suse/ppc/update/6.4/a1/shlibs-2.1.3-154.ppc.rpm
 - ftp://ftp.suse.com/pub/suse/ppc/update/6.4/d1/libc-2.1.3-154.ppc.rpm
 - ftp://ftp.suse.com/pub/suse/ppc/update/6.4/d2/libd-2.1.3-154.ppc.rpm
 - ftp://ftp.suse.com/pub/suse/ppc/update/6.4/zq1/libc-2.1.3-154.src.rpm
- Linux-Mandrake 7.0 et 7.1:
- 7.0/RPMS/glibc-2.1.3-16mdk.i586.rpm
 - 7.0/RPMS/glibc-devel-2.1.3-16mdk.i586.rpm
 - 7.0/RPMS/glibc-profile-2.1.3-16mdk.i586.rpm
 - 7.0/SRPMS/glibc-2.1.3-16mdk.src.rpm
 - 7.1/RPMS/glibc-2.1.3-17mdk.i586.rpm
 - 7.1/RPMS/glibc-devel-2.1.3-17mdk.i586.rpm
 - 7.1/RPMS/glibc-profile-2.1.3-17mdk.i586.rpm
 - 7.1/SRPMS/glibc-2.1.3-17mdk.src.rpm
- Red Hat:
- ftp://updates.redhat.com/5.2/sparc/glibc-2.0.7-29.4.sparc.rpm
 - ftp://updates.redhat.com/5.2/sparc/glibc-debug-2.0.7-29.4.sparc.rpm
 - ftp://updates.redhat.com/5.2/sparc/glibc-devel-2.0.7-29.4.sparc.rpm
 - ftp://updates.redhat.com/5.2/sparc/glibc-profile-2.0.7-29.4.sparc.rpm

- <ftp://updates.redhat.com/5.2/alpha/glibc-2.0.7-29.4.alpha.rpm>
 - <ftp://updates.redhat.com/5.2/alpha/glibc-debug-2.0.7-29.4.alpha.rpm>
 - <ftp://updates.redhat.com/5.2/alpha/glibc-devel-2.0.7-29.4.alpha.rpm>
 - <ftp://updates.redhat.com/5.2/alpha/glibc-profile-2.0.7-29.4.alpha.rpm>
 - <ftp://updates.redhat.com/5.2/i386/glibc-2.0.7-29.4.i386.rpm>
 - <ftp://updates.redhat.com/5.2/i386/glibc-debug-2.0.7-29.4.i386.rpm>
 - <ftp://updates.redhat.com/5.2/i386/glibc-devel-2.0.7-29.4.i386.rpm>
 - <ftp://updates.redhat.com/5.2/i386/glibc-profile-2.0.7-29.4.i386.rpm>
 - <ftp://updates.redhat.com/5.2/SRPMS/glibc-2.0.7-29.4.src.rpm>
 - <ftp://updates.redhat.com/6.2/sparc/glibc-2.1.3-21.sparc.rpm>
 - <ftp://updates.redhat.com/6.2/sparc/glibc-devel-2.1.3-21.sparc.rpm>
 - <ftp://updates.redhat.com/6.2/sparc/glibc-profile-2.1.3-21.sparc.rpm>
 - <ftp://updates.redhat.com/6.2/sparc/nscd-2.1.3-21.sparc.rpm>
 - <ftp://updates.redhat.com/6.2/i386/glibc-2.1.3-21.i386.rpm>
 - <ftp://updates.redhat.com/6.2/i386/glibc-devel-2.1.3-21.i386.rpm>
 - <ftp://updates.redhat.com/6.2/i386/glibc-profile-2.1.3-21.i386.rpm>
 - <ftp://updates.redhat.com/6.2/i386/nscd-2.1.3-21.i386.rpm>
 - <ftp://updates.redhat.com/6.2/alpha/glibc-2.1.3-21.alpha.rpm>
 - <ftp://updates.redhat.com/6.2/alpha/glibc-devel-2.1.3-21.alpha.rpm>
 - <ftp://updates.redhat.com/6.2/alpha/glibc-profile-2.1.3-21.alpha.rpm>
 - <ftp://updates.redhat.com/6.2/alpha/nscd-2.1.3-21.alpha.rpm>
 - <ftp://updates.redhat.com/6.2/sparcv9/glibc-2.1.3-21.sparcv9.rpm>
 - <ftp://updates.redhat.com/6.2/SRPMS/glibc-2.1.3-21.src.rpm>
- TurboLinux:
- <ftp://ftp.turbolinux.com/pub/updates/6.0/glibc-2.1.2-17S.i386.rpm>
 - <ftp://ftp.turbolinux.com/pub/updates/6.0/glibc-2.1.2-15S.i386.rpm>
 - <ftp://ftp.turbolinux.com/pub/updates/6.0/SRPMS/glibc-2.1.2-17S.src.rpm>
 - <ftp://ftp.turbolinux.com/pub/updates/6.0/SRPMS/glibc-2.1.2-15S.src.rpm>

Si votre version d'unix n'est pas citée, veuillez consulter le CERTA.

6 Documentation

- Bulletin de sécurité Debian :
<http://security.debian.org/security/2000/20000902>
- Bulletin de sécurité RedHat :
<http://www.redhat.com/support/errata/RHSA-2000-057-04.html>

Gestion détaillée du document

14 septembre 2000 version initiale.