Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 04 septembre 2000
N° CERTA-2000-AVI-043

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans mgetty sous Unix

Gestion du document

Référence	CERTA-2000-AVI-043
Titre	Vulnérabilité dans mgetty sous Unix
Date de la première version	04 septembre 2000
Date de la dernière version	–
Source(s)	Exploit vérifié par le CERTA Avis du CERT IST
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

Ecrasement de fichiers, modification de la configuration

2 Systèmes affectés

TurboLinux, Linux RedHat, Mandrake et Connectiva, OpenBSD (Caldera) et FreeBSD, AIX, SunOS et Solaris, et tout autre système unix ou linux utilisant mgetty 1.1.21, 1.1.20 ou 1.1.19 développé par Goert Doering installé par défaut ou installé et activé par l'administrateur.

3 Résumé

Un utilitaire de gestion de Fax est installé par défaut sur la plupart des versions de Linux ou Unix. Celle-ci possède une vulnérabilité permettant à un utilisateur local d'écraser des fichiers auxquels il n'a normalement pas accès en écriture.

4 Description

`faxrunqd` est l'outil d'envoie de fax de l'utilitaire *mgetty*. Celui-ci est installé par défaut sur la plupart des Linux ou Unix. Un utilisateur mal intentionné peut détruire des fichiers pour lesquels il n'a pas les droits en écriture à l'aide de `faxrunqd` en utilisant un lien.

Cette vulnérabilité pourait être utilisée, par exemple, pour détruire des fichiers importants, risquant ainsi de compromettre le bon fonctionnement du système ou des documents de travail.

5 Contournement provisoire

Désactiver `faxrunqd`, et éventuellement le supprimer s'il n'est pas utilisé sur la machine concernée.

6 Solution

Appliquer les correctifs en fonction du système concerné :

- Pour Caldera, selon les types et les versions :
  - ftp://ftp.calderasystems.com/pub/updates/OpenLinux/2.3/current/RPMS/mgetty-1.1.22_Aug17-2OL.i386.rpm
  - ftp://ftp.calderasystems.com/pub/updates/OpenLinux/2.3/current/SRPMS/mgetty-1.1.22_Aug17-2OL.src.rpm
  - ftp://ftp.calderasystems.com/pub/updates/eServer/2.3/current/RPMS/mgetty-1.1.22_Aug17-2S.i386.rpm
  - ftp://ftp.calderasystems.com/pub/updates/eServer/2.3/current/SRPMS/SRPMS/mgetty-1.1.22_Aug17-2S.src.rpm
- Pour FreeBSD :
  http://www.FreeBSD.org/cgi/cvsweb.cgi/ports/comms/mgetty%2bsendfax/Makefile
- Pour Connectiva, selon les versions et le type de machine :
  - ftp://atualizacoes.conectiva.com.br/4.0/SRPMS/mgetty-1.1.22-1cl.src.rpm
  - ftp://atualizacoes.conectiva.com.br/4.0/i386/mgetty-1.1.22-1cl.i386.rpm
  - ftp://atualizacoes.conectiva.com.br/4.0/i386/mgetty-sendfax-1.1.22-1cl.i386.rpm
  - ftp://atualizacoes.conectiva.com.br/4.0/i386/mgetty-viewfax-1.1.22-1cl.i386.rpm
  - ftp://atualizacoes.conectiva.com.br/4.0/i386/mgetty-voice-1.1.22-1cl.i386.rpm
  - ftp://atualizacoes.conectiva.com.br/4.0es/SRPMS/mgetty-1.1.22-1cl.src.rpm
  - ftp://atualizacoes.conectiva.com.br/4.0es/i386/mgetty-1.1.22-1cl.i386.rpm
  - ftp://atualizacoes.conectiva.com.br/4.0es/i386/mgetty-sendfax-1.1.22-1cl.i386.rpm
  - ftp://atualizacoes.conectiva.com.br/4.0es/i386/mgetty-viewfax-1.1.22-1cl.i386.rpm
  - ftp://atualizacoes.conectiva.com.br/4.0es/i386/mgetty-voice-1.1.22-1cl.i386.rpm
  - ftp://atualizacoes.conectiva.com.br/4.1/SRPMS/mgetty-1.1.22-1cl.src.rpm
  - ftp://atualizacoes.conectiva.com.br/4.1/i386/mgetty-1.1.22-1cl.i386.rpm
  - ftp://atualizacoes.conectiva.com.br/4.1/i386/mgetty-sendfax-1.1.22-1cl.i386.rpm
  - ftp://atualizacoes.conectiva.com.br/4.1/i386/mgetty-viewfax-1.1.22-1cl.i386.rpm
  - ftp://atualizacoes.conectiva.com.br/4.1/i386/mgetty-voice-1.1.22-1cl.i386.rpm
  - ftp://atualizacoes.conectiva.com.br/4.2/SRPMS/mgetty-1.1.22-1cl.src.rpm
  - ftp://atualizacoes.conectiva.com.br/4.2/i386/mgetty-1.1.22-1cl.i386.rpm
  - ftp://atualizacoes.conectiva.com.br/4.2/i386/mgetty-sendfax-1.1.22-1cl.i386.rpm
  - ftp://atualizacoes.conectiva.com.br/4.2/i386/mgetty-viewfax-1.1.22-1cl.i386.rpm
  - ftp://atualizacoes.conectiva.com.br/4.2/i386/mgetty-voice-1.1.22-1cl.i386.rpm
  - ftp://atualizacoes.conectiva.com.br/5.0/SRPMS/mgetty-1.1.22-1cl.src.rpm
  - ftp://atualizacoes.conectiva.com.br/5.0/i386/mgetty-1.1.22-1cl.i386.rpm
  - ftp://atualizacoes.conectiva.com.br/5.0/i386/mgetty-sendfax-1.1.22-1cl.i386.rpm

  - ftp://atualizacoes.conectiva.com.br/5.0/i386/mgetty-viewfax-1.1.22-1cl.i386.rpm
  - ftp://atualizacoes.conectiva.com.br/5.0/i386/mgetty-voice-1.1.22-1cl.i386.rpm
  - ftp://atualizacoes.conectiva.com.br/5.1/SRPMS/mgetty-1.1.22-1cl.src.rpm
  - ftp://atualizacoes.conectiva.com.br/5.1/i386/mgetty-1.1.22-1cl.i386.rpm
  - ftp://atualizacoes.conectiva.com.br/5.1/i386/mgetty-sendfax-1.1.22-1cl.i386.rpm
  - ftp://atualizacoes.conectiva.com.br/5.1/i386/mgetty-viewfax-1.1.22-1cl.i386.rpm
  - ftp://atualizacoes.conectiva.com.br/5.1/i386/mgetty-voice-1.1.22-1cl.i386.rpm
  - ftp://atualizacoes.conectiva.com.br/ferramentas/ecommerce/SRPMS/mgetty-1.1.22-1cl.src.rpm
  - ftp://atualizacoes.conectiva.com.br/ferramentas/ecommerce/i386/mgetty-1.1.22-1cl.i386.rpm
  - ftp://atualizacoes.conectiva.com.br/ferramentas/ecommerce/i386/mgetty-sendfax-1.1.22-1cl.i386.rpm
  - ftp://atualizacoes.conectiva.com.br/ferramentas/ecommerce/i386/mgetty-viewfax-1.1.22-1cl.i386.rpm
  - ftp://atualizacoes.conectiva.com.br/ferramentas/ecommerce/i386/mgetty-voice-1.1.22-1cl.i386.rpm
  - ftp://atualizacoes.conectiva.com.br/ferramentas/graficas/SRPMS/mgetty-1.1.22-1cl.src.rpm
  - ftp://atualizacoes.conectiva.com.br/ferramentas/graficas/i386/mgetty-1.1.22-1cl.i386.rpm
  - ftp://atualizacoes.conectiva.com.br/ferramentas/graficas/i386/mgetty-sendfax-1.1.22-1cl.i386.rpm
  - ftp://atualizacoes.conectiva.com.br/ferramentas/graficas/i386/mgetty-viewfax-1.1.22-1cl.i386.rpm
  - ftp://atualizacoes.conectiva.com.br/ferramentas/graficas/i386/mgetty-voice-1.1.22-1cl.i386.rpm
- Mandrake selon les versions :
  Sur les sites FTP mirroirs de la liste :
  http://www.linux-mandrake.com/en/ftp.php3 ,dans les répertoires dont le chemin varie selon la version :
  - 6.0/RPMS/mgetty-1.1.22-2mdk.i586.rpm
  - 6.0/RPMS/mgetty-contrib-1.1.22-2mdk.i586.rpm
  - 6.0/RPMS/mgetty-sendfax-1.1.22-2mdk.i586.rpm
  - 6.0/RPMS/mgetty-viewfax-1.1.22-2mdk.i586.rpm
  - 6.0/RPMS/mgetty-voice-1.1.22-2mdk.i586.rpm
  - 6.0/SRPMS/mgetty-1.1.22-2mdk.src.rpm
  - 6.1/RPMS/mgetty-1.1.22-2mdk.i586.rpm
  - 6.1/RPMS/mgetty-contrib-1.1.22-2mdk.i586.rpm
  - 6.1/RPMS/mgetty-sendfax-1.1.22-2mdk.i586.rpm
  - 6.1/RPMS/mgetty-viewfax-1.1.22-2mdk.i586.rpm
  - 6.1/RPMS/mgetty-voice-1.1.22-2mdk.i586.rpm
  - 6.1/SRPMS/mgetty-1.1.22-2mdk.src.rpm
  - 7.0/RPMS/mgetty-1.1.22-2mdk.i586.rpm
  - 7.0/RPMS/mgetty-contrib-1.1.22-2mdk.i586.rpm
  - 7.0/RPMS/mgetty-sendfax-1.1.22-2mdk.i586.rpm
  - 7.0/RPMS/mgetty-viewfax-1.1.22-2mdk.i586.rpm
  - 7.0/RPMS/mgetty-voice-1.1.22-2mdk.i586.rpm
  - 7.0/SRPMS/mgetty-1.1.22-2mdk.src.rpm
  - 7.1/RPMS/mgetty-1.1.22-2mdk.i586.rpm
  - 7.1/RPMS/mgetty-contrib-1.1.22-2mdk.i586.rpm
  - 7.1/RPMS/mgetty-sendfax-1.1.22-2mdk.i586.rpm
  - 7.1/RPMS/mgetty-viewfax-1.1.22-2mdk.i586.rpm
  - 7.1/RPMS/mgetty-voice-1.1.22-2mdk.i586.rpm
  - 7.1/SRPMS/mgetty-1.1.22-2mdk.src.rpm
- Pour savoir s'il existe une mise à jour de mgetty pour les autres systèmes contacter les éditeurs.

7 Documentation

- Avis de sécurité de Caldera :
  http://www.calderasystems.com/support/security/advisories/CSSA-200-029.0.txt
- Avis de sécurité de Mandrake :
  http://www.linux-mandrake.com/en/fupdate.php3

Gestion détaillée du document

04 septembre 2000 version initiale.