



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 20 septembre 2000
N° CERTA-2000-AVI-050

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le démon klogd 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-050>

Gestion du document

Référence	CERTA-2000-AVI-050
Titre	Vulnérabilité dans le démon klogd sous Linux
Date de la première version	20 septembre 2000
Date de la dernière version	–
Source(s)	BugTraq Avis de sécurité Red Hat Avis de sécurité Mandrake Avis de sécurité Debian
Pièce(s) jointe(s)	Aucune

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

1 Risque

Exécution de code arbitraire permettant l'accès aux privilèges *root* en local.
Accès *root* distant possible mais non démontré.

2 Systèmes affectés

Toute distribution Linux (Red Hat, Mandrake, Debian, Slackware,...) pour tout processeur.

3 Résumé

Le démon *klogd*, chargé de journaliser les messages du noyau, comporte une vulnérabilité qui peut être exploitée par un utilisateur local pour obtenir les privilèges du super-utilisateur.

4 Description

Le démon *klogd* lit les messages émis par le noyau, reformate ces messages et les transmet au démon *syslogd* qui les stocke dans divers journaux selon la configuration donnée par le fichier *syslog.conf*. La procédure de ré-

écriture de ces messages ne gère pas correctement tous les symboles possibles. Des chaînes de caractères peuvent alors être fabriquées pour tuer le démon *klogd* voire lui faire exécuter du code arbitraire.

Il n'y a pas besoin d'être super-utilisateur pour faire émettre un message par le noyau. Par exemple, la mauvaise initialisation d'une socket provoque un message du noyau incluant le nom du programme, donnée qui peut être falsifiée. Il est également possible de développer un gestionnaire malicieux pour certains périphériques qui sont accessibles en lecture pour tout le monde...

5 Solution

Mettre à jour le paquetage *klogd/syslogd* en fonction de la distribution utilisée.

5.1 Red Hat

5.1.1 Version 5.2

Sources <ftp://updates.redhat.com/5.2/SRPMS/sysklogd-1.3.31-1.6.src.rpm>

Intel 386 <ftp://updates.redhat.com/5.2/i386/sysklogd-1.3.31-1.6.i386.rpm>

Sparc <ftp://updates.redhat.com/5.2/sparc/sysklogd-1.3.31-1.6.sparc.rpm>

Alpha <ftp://updates.redhat.com/5.2/alpha/sysklogd-1.3.31-1.6.alpha.rpm>

5.1.2 Version 6.2

Sources <ftp://updates.redhat.com/6.2/SRPMS/sysklogd-1.3.31-17.src.rpm>

Intel 386 <ftp://updates.redhat.com/6.2/i386/sysklogd-1.3.31-17.i386.rpm>

Sparc <ftp://updates.redhat.com/6.2/sparc/sysklogd-1.3.31-17.sparc.rpm>

Alpha <ftp://updates.redhat.com/6.2/alpha/sysklogd-1.3.31-17.alpha.rpm>

5.2 Mandrake

5.2.1 Version 6.0

Sources ftp://ftp.free.fr/pub/Distributions_Linux/Mandrake/updates/6.0/SRPMS/sysklogd-1.3.31-14mdk.src.rpm

Intel Pentium ftp://ftp.free.fr/pub/Distributions_Linux/Mandrake/updates/6.0/RPMS/sysklogd-1.3.31-14mdk.i586.rpm

5.2.2 Version 6.1

Sources ftp://ftp.free.fr/pub/Distributions_Linux/Mandrake/updates/6.1/SRPMS/sysklogd-1.3.31-14mdk.src.rpm

Intel Pentium ftp://ftp.free.fr/pub/Distributions_Linux/Mandrake/updates/6.1/RPMS/sysklogd-1.3.31-14mdk.i586.rpm

5.2.3 Version 7.0

Sources ftp://ftp.free.fr/pub/Distributions_Linux/Mandrake/updates/7.0/SRPMS/sysklogd-1.3.31-15mdk.src.rpm

Intel Pentium ftp://ftp.free.fr/pub/Distributions_Linux/Mandrake/updates/7.0/RPMS/sysklogd-1.3.31-15mdk.i586.rpm

5.2.4 Version 7.1

Sources ftp://ftp.free.fr/pub/Distributions_Linux/Mandrake/updates/7.1/SRPMS/sysklogd-1.3.31-15mdk.src.rpm

Intel Pentium ftp://ftp.free.fr/pub/Distributions_Linux/Mandrake/updates/7.1/RPMS/sysklogd-1.3.31-15mdk.i586.rpm

5.3 Caldera

5.3.1 OpenLinux Desktop 2.3

Sources <ftp://ftp.calderasystems.com/pub/updates/OpenLinux/2.3/current/SRPMS/sysklogd-1.4-2.src.rpm>

Intel 386 <ftp://ftp.calderasystems.com/pub/updates/OpenLinux/2.3/current/RPMS/sysklogd-1.4-2.i386.rpm>

5.3.2 OpenLinux eServer 2.3 et OpenLinux eBuilder for ECential 3.0

Sources <ftp://ftp.calderasystems.com/pub/updates/eServer/2.3/current/SRPMS/sysklogd-1.4-2.src.rpm>

Intel 386 <ftp://ftp.calderasystems.com/pub/updates/eServer/2.3/current/RPMS/sysklogd-1.4-2.i386.rpm>

5.3.3 OpenLinux eDesktop 2.4

Sources <ftp://ftp.calderasystems.com/pub/updates/eDesktop/2.4/current/SRPMS/sysklogd-1.4-2.src.rpm>

Intel 386 <ftp://ftp.calderasystems.com/pub/updates/eDesktop/2.4/current/RPMS/sysklogd-1.4-2.i386.rpm>

5.4 Slackware

<ftp://ftp.slackware.com/pub/slackware/slackware-current/slakware/a1/sysklogd.tgz>

5.5 Debian

5.5.1 Version 2.1 (slink)

Sources http://security.debian.org/dists/slink/updates/source/sysklogd_1.3.orig.tar.gz
et
http://security.debian.org/dists/slink/updates/source/sysklogd_1.3-31.slink1.diff.gz

Intel 386 http://security.debian.org/dists/slink/updates/binary-i386/sysklogd_1.3-31.slink1_i386.deb

5.5.2 Version 2.2 (potato)

Sources http://security.debian.org/dists/potato/updates/main/source/sysklogd_1.3.orig.tar.gz
et
http://security.debian.org/dists/potato/updates/main/source/sysklogd_1.3-33.1.diff.gz

Intel 386 http://security.debian.org/dists/potato/updates/main/binary-i386/sysklogd_1.3-33.1_i386.deb

Sparc http://security.debian.org/dists/potato/updates/main/binary-sparc/sysklogd_1.3-33.1_sparc.deb

Alpha http://security.debian.org/dists/potato/updates/main/binary-alpha/sysklogd_1.3-33.1_alpha.deb

Arm http://security.debian.org/dists/potato/updates/main/binary-arm/sysklogd_1.3-33.1_arm.deb

5.6 Immunix

Sources http://www.immunix.org:8080/ImmunixOS/6.2/updates/SRPMS/sysklogd-1.3.31-17_StackGuard.src.rpm

Intel **386** http://www.immunix.org:8080/ImmunixOS/6.2/updates/RPMS/sysklogd-1.3.31-17_StackGuard.i386.rpm

5.7 Trustix

<ftp://ftp.trustix.com/pub/Trustix/updates/1.1/RPMS/sysklogd-1.3.31-18tr.i586.rpm>

6 Documentation

- Avis de sécurité Red Hat
<http://www.red-hat.com/support/errata/RHSA-2000-061-02.html>
- Avis de sécurité Mandrake
<http://www.linux-mandrake.com/en/security/MDKSA-2000-050.php3>
- Avis de sécurité Caldera
<http://www.calderasystems.com/support/security/advisories/CSSA-2000-032.0.txt>

Gestion détaillée du document

20 septembre 2000 version initiale.