

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans l'utilitaire makewhatis 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-AVI-014>

Gestion du document

Référence	CERTA-2000-AVI-014
Titre	Vulnérabilité dans l'utilitaire makewhatis sous Unix
Date de la première version	13 juillet 2000
Date de la dernière version	–
Source(s)	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

Contournement des règles de sécurité et à terme, accès root.

2 Systèmes affectés

- Linux RedHat 5.2 et 6.2 ayant l'utilitaire « makewhatis »,
- Linux Caldera.

3 Résumé

L'utilitaire « makewhatis » est utilisé sous unix pour mettre à jour les bases de données utilisées par les commandes whatis et apropos. Redhat a trouvé une vulnérabilité qui permet à un utilisateur local de modifier des fichiers auquel il n'a normalement pas accès. L'utilisateur mal intentionné pourrait augmenter ses privilèges en tirant partie de cette vulnérabilité.

4 Description

L'utilitaire makewhatis génère des fichiers temporaires dont les noms sont prévisibles. En appliquant les méthodes d'attaques utilisant des liens symboliques, l'utilisateur mal intentionné peut détourner l'usage du script makewhatis afin de modifier des fichiers, les renommer, ou en changer les permissions.

5 Solution

Redhat recommande de mettre à jour makewhatis avec les correctifs proposés aux adresses suivantes :

– Red Hat Linux 5.2 :

i386 <ftp://updates.redhat.com/5.2/i386/man-1.5h1-2.5.x.i386.rpm>

alpha <ftp://updates.redhat.com/5.2/alpha/man-1.5h1-2.5.x.alpha.rpm>

sparc <ftp://updates.redhat.com/5.2/sparc/man-1.5h1-2.5.x.sparc.rpm>

– Red Hat Linux 6.2 :

alpha <ftp://updates.redhat.com/6.2/alpha/man-1.5h1-2.6.x.alpha.rpm>

i386 <ftp://updates.redhat.com/6.2/i386/man-1.5h1-2.6.x.i386.rpm>

sparc <ftp://updates.redhat.com/6.2/sparc/man-1.5h1-2.6.x.sparc.rpm>

– Caldera :

– <ftp://ftp.calderasystems.com/pub/updates/OpenLinux/2.3/current/RPMS/man-1.5f-6.i386.rpm>

– <ftp://ftp.calderasystems.com/pub/updates/OpenLinux/2.3/current/SRPMS/man-1.5f-6.src.rpm>

– <ftp://ftp.calderasystems.com/pub/updates/eServer/2.3/current/RPMS/man-1.5f-6.i386.rpm>

– <ftp://ftp.calderasystems.com/pub/updates/eServer/2.3/current/SRPMS/man-1.5f-6.src.rpm>

– <ftp://ftp.calderasystems.com/pub/updates/eDesktop/2.4/current/RPMS/man-1.5g-2.i386.rpm>

– <ftp://ftp.calderasystems.com/pub/updates/eDesktop/2.4/current/SRPMS/man-1.5g-2.src.rpm>

Pour chaque fichier RPM exécuter la commande :

```
rpm -Fvh nom_du_fichier.rpm
```

6 Documentation

Avis de Sécurité RedHat :

<http://www.redhat.com/support/errata/RHSA-2000-041-02.html>

Gestion détaillée du document

13 juillet 2000 version initiale.