Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 22 août 2000
N° CERTA-2000-AVI-033

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans GNOME Updater

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-033

Gestion du document

Référence	CERTA-2000-AVI-033
Titre	Vulnérabilité dans GNOME Updater
Date de la première version	22 août 2000
Date de la dernière version	–
Source(s)	Helix Code (Developpeurs de GNOME) SecurityFocus
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

Usurpation de privilèges root.

2 Systèmes affectés

Helix Code Updater 0.1 à 0.5 pour les sytèmes TurboLinux 6.0.4, SuSE linux 6.3 et 6.4, Redhat Linux 6.2i386,Mandrake Linux 7.1 , Linux Caldera Desktop 2.4, et Sun Solaris.

3 Résumé

GNOME est un environnement graphique pour X11 développé par Helix Code, et est fourni avec de nombreuses distributions de Linux bien connues.

Le logiciel de mise à jour de GNOME présente une vulnérabilité permettant à un utilisateur local d'augmenter ses privilèges grâce à une intervention sur les fichiers intervenant dans le processus de mise à jour de l'environnement.

4 Description

Le logiciel de mise à jour de GNOME (*Helix Code Updater*) utilise le format de fichier RPM qui extrait ses fichiers dans le répertoire `/tmp/helix-install`. Le répertoire `/tmp` a la particularité d'être accessible en écriture pour tout les utilisateurs du système. Un utilisateur local mal intentionné peut y installer au préalable un répertoire `helix-install` de sa conception contenant des fichiers RPM lui permettant d'élever ses privilèges.

5 Solution

La version 0.6 de Helix Code Updater corrige cette vulnérabilité en écrivant le répertoire `helix-install` dans le répertoire `/var/cache` dont les permissions permettent un accès en écriture par root uniquement.

La liste des plate-formes et versions supportant cette version se trouve à l'adresses suivante :
http://www.helixcode.com/desktop/download.php3

Sinon, mettez à jour la version de Helix Code Updater selon le système que vous possédez :

- TurboLinux :
  http://spidermonkey.helixcode.com/distributions/TurboLinux-6/helix-update-0.6-0_helix_3.i386.rpm
- Caldera OpenLinux eDesktop systems:
  http://spidermonkey.helixcode.com/distributions/Caldera-2.4/helix-update-0.6-0_helix_2.i386.rpm
- LinuxPPC :
  http://spidermonkey.helixcode.com/distributions/LinuxPPC/helix-update-0.6.0_helix_2.ppc.rpm
- Linux Mandrake :
  http://spidermonkey.helixcode.com/distributions/Mandrake/helix-update-0.6-0mdk_helix_2.i586.rpm
- Red Hat Linux :
  http://spidermonkey.helixcode.com/distributions/RedHat-6/helix-update-0.6-0_helix_2.i386.rpm
- Solaris :
  http://spidermonkey.helixcode.com/distributions/Solaris/helix-update-0.6-0_helix_1.sparc64.rpm
- SuSE 6.3 :
  http://spidermonkey.helixcode.com/distributions/SuSE/hupdate-0.6-0_helix_2.i386.rpm
- SuSE 6.4 :
  http://spidermonkey.helixcode.com/distributions/SuSE-6.4/hupdate-0.6-0_helix_2.i386.rpm

6 Documentation

Avis de Helix Code :
http://securityfocus.com/templates/advisory.html?id=2534

Gestion détaillée du document

22 août 2000 version initiale.