Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 26 mars 2003
N° CERTA-2003-AVI-063

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités de Ximian Evolution

Gestion du document

Référence	CERTA-2003-AVI-063
Titre	Vulnérabilités de Ximian Evolution
Date de la première version	26 mars 2003
Date de la dernière version	–
Source(s)	Avis de CoreSecurity CORE-20030304-01
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

- Déni de service ;
- exécution de code arbitraire ;
- contournement de règles de sécurité.

2 Systèmes affectés

Ximian Evolution versions 1.2.2 et antérieures.

3 Résumé

Le client mél Ximian Evolution présente trois vulnérabilités qui permettent à un utilisateur mal intentionné d'exécuter du code arbitraire ou de provoquer un déni de service.

4 Description

Deux vulnérabilités concernent le codage *UUEncode*. La première permet, en construisant malicieusement un en-tête *UUEncode*, de provoquer l'arrêt brutal de l'application Evolution. La deuxième permet de provoquer un

déni de service sur le système en utilisant plusieurs codages *UUEncode* itératifs.

Une autre vulnérabilité concerne certains fichiers au format MIME. Il est possible d'y inclure un code arbitraire qui sera exécuté par le système vulnérable.

5 Solution

Installer la version 1.2.3 de Ximian Evolution :
http://www.ximian.com

ou consulter l'éditeur pour connaître la disponibilité des correctifs :

- avis de sécurité RedHat RHSA-2003:108-16 :
  http://rhn.redhat.com/errata/RHSA-2003-108.html

- avis de sécurité Gentoo :
  http://forums.gentoo.org/viewtopic.php?t=42816

6 Documentation

Avis de sécurité CoreSecurity CORE-20030304-01 :
http://www.coresecurity.com/common/showdoc.php?idx=309&idxseccion=10

Référence CVE CAN-2003-0128 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0128

Référence CVE CAN-2003-0129 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0129

Référence CVE CAN-2003-0130 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0130

Gestion détaillée du document

26 mars 2003 version initiale.