



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 septembre 2005
N° CERTA-2005-AVI-314-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité d'Evolution

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-2005-AVI-314>

Gestion du document

Référence	CERTA-2005-AVI-314-002
Titre	Vulnérabilité d'Evolution
Date de la première version	16 août 2005
Date de la dernière version	24 mars 2006
Source(s)	Bulletin de sécurité SA05-001 du SITIC
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

Exécution de code arbitraire à distance.

2 Systèmes affectés

- Evolution versions 1.5, 2.0, 2.1, 2.2 et 2.3 jusqu'à 2.3.6.1 ;
- la version 2.3.7 d'Evolution n'est pas vulnérable.

3 Description

Evolution est un logiciel qui offre aux utilisateurs de l'environnement de bureau GNOME l'intégration d'un courrier électronique, la gestion d'un carnet d'adresse et d'un calendrier.

Une vCard est l'équivalent numérique d'une carte de visite.

Plusieurs vulnérabilités de type *format string* affectent les versions vulnérables du logiciel Evolution :

- la visualisation des vCards est vulnérable. Un utilisateur mal intentionné peut confectionner une vCard astucieusement construite et l'envoyer par courriel sous la forme d'une pièce jointe. Lorsque l'utilisateur d'une version vulnérable d'Evolution cliquera pour voir l'affichage complet d'une vCard dans un message ou dans le carnet d'adresse, il risque d'exécuter à son insu du code arbitraire ;

- la visualisation des données de contact issues d'un serveur LDAP distant est vulnérable ;
- la visualisation des données d'une « liste de tâches » provenant d'un serveur distant est vulnérable ;
- d'autres vulnérabilités de ce type affectent la gestion du calendrier.

4 Contournement provisoire

La version 2.3.7 du logiciel `Evolution` n'est pas vulnérable. Il s'agit cependant d'une version expérimentale.

5 Solution

Appliquer les correctifs des vendeurs de logiciel.

6 Documentation

- Le bulletin de sécurité du SITIC :
http://www.sitic.se/eng/advisories_and_recommendations/sa05-001.html
- Site Internet du logiciel `Evolution` :
<http://www.gnome.org/projects/evolution>
- Mises à jour de sécurité Fedora :
 - Fedora Core 3 :
<http://www.redhat.com/archives/fedora-announce-list/2005-August/msg0030.html>
 - Fedora Core 4 :
<http://www.redhat.com/archives/fedora-announce-list/2005-August/msg0031.html>
- Bulletin de sécurité Mandriva MDKSA-2005:141 du 17 août 2005 :
<http://www.mandriva.com/security/advisories?name=MDKSA-2005:141>
- Bulletin de sécurité RedHat RHSA-2005:267 du 29 août 2005 :
<http://rhn.redhat.com/errata/RHSA-2005-267.html>
- Bulletin de sécurité SUSE SUSE-SA:2005:054 du 16 septembre 2005 :
http://www.novell.com/linux/security/advisories/2005_54_evolution.html
- Bulletin de sécurité Debian DSA-1016 du 23 mars 2006 :
<http://www.debian.org/security/2006/dsa-1016>
- Référence CVE CAN-2005-2549 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2549>
- Référence CVE CAN-2005-2550 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2550>

Gestion détaillée du document

16 août 2005 version initiale.

26 septembre 2005 ajout des références aux bulletins de sécurité Mandriva MDKSA-2005:141, RedHat RHSA-2005:743 et SUSE SUSE-SA:2005:054 ainsi qu'aux références CVE CAN-2005-2549 et CAN-2005-2550.

24 mars 2006 ajout de la référence au bulletin de sécurité Debian DSA-1016.