



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 4 novembre 2002
N° CERTA-2002-AVI-243

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : uudecode ne vérifie pas les liens symboliques

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-2002-AVI-243>

Gestion du document

Référence	CERTA-2002-AVI-243
Titre	uudecode ne vérifie pas les liens symboliques
Date de la première version	4 novembre 2002
Date de la dernière version	–
Source(s)	CERT CC : Vulnerability Note Vu#336083 CVE : CAN-2002-0178 RedHat : RHSA-2002:065 Avis OpenLinux : CSSA-2002-040.0 Mandrake : MDKSA-2002:052
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

Un utilisateur local peut occasionner des :

- pertes de données ;
- dénis de service ;
- élévations de privilèges.

2 Systèmes affectés

- Mandrake ;
- RedHat ;
- OpenLinux.

3 Résumé

Une vulnérabilité du logiciel `uudecode` permet d'écraser des fichiers, conduisant dans certains cas à une élévation de privilèges.

4 Description

Le mél (SMTP) et les forums de discussion sur Internet (NNTP) ont été conçus pour échanger des messages textuels en anglais. De nombreux systèmes ont donc été conçus pour échanger des messages ne contenant que des caractères imprimables du jeu ASCII. En pratique 7 bits suffisent pour représenter chaque caractère (le bit de poids fort de chaque octet est nul).

Lorsqu'il faut échanger des textes avec des caractères accentués ou bien des pièces jointes (images, sons, ...) ces systèmes ne fonctionnent plus, car ils sont confrontés à des octets dont le bit de poids fort vaut 1.

Un contournement de cette limitation est d'*encoder* les données binaires en un ensemble de caractères ASCII avant de les émettre. Une des normes pour réaliser ce type d'encodage est `uuencode` (*Unix to Unix encode*).

Par exemple, l'encodage d'une image :

```
begin 644 toto.gif
M1TE&. #EA=P!/\<`. (M,>,N,.,N,M\N,N$O,>(Q-. (Q,N,R,^(I+MPH+N(J
[... ]
ME!`;%1([L4U1L1:;!B;L46QL1P;%![[L4;A3"*+%2%;LCMQLBA[$RJ[LDI!
8LBY[L3`;LQK[$#8*>[,XF[,ZZQ`!`0`[
`
end
```

où `toto.gif` désigne le nom du fichier à créer lorsque la pièce jointe sera décodée par le logiciel `uudecode`.

Le paquetage GNU `Sharutils` est un ensemble de logiciels destinés à faire des *archives shell* pour la transmission de données par le mél. Parmi les logiciels de ce paquetage, on trouve une implémentation du logiciel `uudecode`.

Cette implémentation d'`uudecode` ne vérifie pas, avant d'écrire le fichier décodé sur le disque, si le fichier existe déjà et notamment s'il n'est pas un lien ou un tube nommé.

Ceci permet une attaque classique d'écrasement de fichiers en suivant les liens symboliques. Cette technique peut permettre dans certains cas une élévation de privilèges d'un utilisateur local.

D'autres implémentations de `uudecode` peuvent être touchées par cette vulnérabilité. La page du *CERT Coordination Center* précise quelles sont les implémentations vulnérables connues.

5 Solution

Appliquer le correctif proposé pour les implémentations vulnérables. Les avis de sécurité suivants précisent des implémentations à corriger :

RedHat avis RHTSA-2002:065

OpenLinux avis CSSA-2002-040.0

Mandrake avis MDKSA-2002:052

6 Documentation

- Page d'accueil du projet GNU `Sharutils` :
<http://www.gnu.org/software/sharutils/sharutils.html> ;
- description de la vulnérabilité et des implémentations vulnérables connues sur la page du *CERT Coordination Center* :
<http://www.kb.cert.org/vuls/id/336083>
- avis OpenLinux
<http://www.sco.com/support/security>
- avis RedHat
<http://rhn.redhat.com/errata>
- avis Mandrake
<http://www.mandrakesecure.net/archives/2002-08/msg00003.php>

Gestion détaillée du document

4 novembre 2002 version initiale.