

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de GNU encript

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-070>

Gestion du document

Référence	CERTA-2005-AVI-070-002
Titre	Vulnérabilité de GNU encript
Date de la première version	14 février 2005
Date de la dernière version	17 février 2005
Source(s)	Bulletin de sécurité Debian DSA-654 du 21 janvier 2005
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.

2 Systèmes affectés

GNU `encript` version 1.6.4 et versions antérieures.

3 Description

GNU `encript` est un logiciel libre qui permet de transformer des fichiers du format ASCII au format Post-script.

Plusieurs vulnérabilités dans GNU `encript` permettent à un utilisateur mal intentionné de faire exécuter du code arbitraire sur la plate-forme vulnérable.

4 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

5 Documentation

- Site Internet de GNU `enscript` :
<http://people.ssh.com/mtr/genscript>
- Bulletin de sécurité Debian DSA-654 du 21 janvier 2005 :
<http://www.debian.org/security/2005/dsa-654>
- Bulletin de sécurité RedHat RHSA-2005:039 du 01 février 2005 :
<http://rhn.redhat.com/errata/RHSA-2005-039.html>
- Bulletin de sécurité RedHat RHSA-2005:040 du 15 février 2005 :
<http://rhn.redhat.com/errata/RHSA-2005-040.html>
- Bulletin de sécurité Gentoo GLSA 200502-03 du 02 février 2005 :
<http://www.gentoo.org/security/en/glsa/glsa-200502-03.xml>
- Bulletin de sécurité Mandrake MDKSA-2005:033 du 10 février 2005 :
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2005:033>
- Bulletin de sécurité OpenBSD pour `enscript` du 11 février 2005 :
<http://www.vuxml.org/openbsd/>
- Bulletin de sécurité FreeBSD pour `enscript-a4`, `enscript-letter` et `enscript-letterdj` du 11 février 2005 :
<http://www.vuxml.org/freebsd/>
- Bulletin de sécurité SGI 20050202-01-U du 09 février 2005 :
<ftp://patches.sgi.com/support/free/security/advisories/20050202-01-U.asc>
- Référence CVE CAN-2004-1184 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1184>
- Référence CVE CAN-2004-1185 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1185>
- Référence CVE CAN-2004-1186 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1186>

Gestion détaillée du document

14 février 2005 version initiale.

14 février 2005 ajout de la référence au bulletin de sécurité SGI 20050202-01-U.

17 février 2005 ajout de la référence au bulletin de sécurité RedHat RHSA-2005:040.