

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans le paquetage Netpbm

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-2003-AVI-061>

Gestion du document

Référence	CERTA-2003-AVI-061-001
Titre	Multiples vulnérabilités dans le paquetage Netpbm
Date de la première version	26 mars 2003
Date de la dernière version	04 avril 2003
Source(s)	Bulletin de sécurité DSA-263 de Debian Bulletin de sécurité MDKSA-2003:036 de Mandrake
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 ;
- déni de service.

2 Systèmes affectés

Versions de Netpbm antérieures ou égales à 10.14.

3 Résumé

De multiples vulnérabilités ont été découvertes dans le paquetage Netpbm.

4 Description

Netpbm est un paquetage comprenant une bibliothèque et des outils utilisés pour la manipulation d'images de différents formats.

De multiples vulnérabilités de type débordement de mémoire sont présentes dans le paquetage Netpbm.
Au moyen d'une image habilement constituée, un utilisateur mal intentionné peut exploiter ces vulnérabilités à travers une application utilisant ce paquetage afin d'exécuter du code arbitraire ou réaliser un déni de service.

5 Solution

Appliquer le correctif selon l'éditeur :

- Bulletin de sécurité DSA-263 "netpbm-free – math overflow errors" de Debian :
<http://www.debian.org/security/2003/dsa-263>
- Bulletin de sécurité MDKSA-2003:036 "netpbm" de Mandrake :
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2003:036>
- Bulletin de sécurité RHSA-2003:060 de Red Hat :
<http://rhn.redhat.com/errata/RHSA-2003-060.html>
- Bulletin de sécurité RHSA-2003:061 de Red Hat :
<http://rhn.redhat.com/errata/RHSA-2003-061.html>

6 Documentation

- Document "Arithmetic overflows in Netpbm" sur le site de Netpbm :
<http://netpbm.sourceforge.net/overflow.html>
- Référence CVE CAN-2003-0146 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0146>

Gestion détaillée du document

26 mars 2003 version initiale.

4 avril 2003 ajout références aux bulletins de sécurité de Red Hat.