Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 21 décembre 2005
N° CERTA-2005-AVI-466-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Netpbm

Gestion du document

Référence	CERTA-2005-AVI-466-002
Titre	Vulnérabilité de Netpbm
Date de la première version	22 novembre 2005
Date de la dernière version	21 décembre 2005
Source(s)	Bulletin de sécurité Debian DSA-904 du 21 novembre 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

- Déni de service ;
- exécution de code arbitraire.

2 Systèmes affectés

Toutes les versions de `pnmtopng / pngtopnm` antérieures à la version 2.39.

3 Résumé

Une vulnérabilité dans Netpbm permet à un utilisateur mal intentionné de réaliser un déni de service ou d'exécuter du code arbitraire à distance sur la plate-forme vulnérable.

4 Description

Netpbm est un ensemble d'outils de conversions graphiques.
Plusieurs vulnérabilités de type débordement de mémoire dans l'outil `pnmtopng` permettent à un utilisateur mal intentionné de réaliser un déni de service ou d'exécuter du code arbitraire à distance au moyen d'un fichier PNM malicieusement construit.

5 Solution

Mettre à jour `pnmtopng / pngtopnm` en version 2.39.
Dans tous les cas se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Site Internet de Netpbm :
  http://netpbm.sourceforge.net/
- Sortie de la nouvelle version de `pnmtopng / pngtopnm` :
  http://sourceforge.net/project/shownotes.php?release_id=370545
- Bulletin de sécurité Debian DSA-904 du 21 novembre 2005 :
  http://www.debian.org/security/2005/dsa-904
- Bulletin de sécurité Mandriva MDKSA-2005:217 du 30 novembre 2005 :
  http://frontal2.mandriva.com/security/advisories?name=MDKSA-2005:217
- Bulletin de sécurité RedHat RHSA-2005:843 du 20 décembre 2005 :
  http://rhn.redhat.com/errata/RHSA-2005-843.html
- Référence CVE CAN-2005-3632 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-3632
- Référence CVE CAN-2005-3662 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-3662

Gestion détaillée du document

22 novembre 2005 version initiale.
01 décembre 2005 ajout de la référence au bulletin de sécurité Mandriva MDKSA-2005:217.
21 décembre 2005 ajout de la référence au bulletin de sécurité RedHat RHSA-2005:843.