Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 12 Mai 2003
N° CERTA-2003-AVI-031-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du serveur VNC et TightVNC

Gestion du document

Référence	CERTA-2003-AVI-031-001
Titre	Vulnérabilité du serveur VNC et TightVNC
Date de la première version	28 février 2003
Date de la dernière version	12 mai 2003
Source(s)	Avis de sécurité RedHat RHSA-2003:041-12
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

- Contournement de la politique de sécurité ;
- contrôle de la machine à distance.

2 Systèmes affectés

- Selon la distribution GNU/Linux, les versions vulnérables de VNC sont :
  - RedHat et Mandrake : toutes les versions de VNC antérieures à la version 3.3.3r2 ;
  - Gentoo : toutes les versions de VNC antérieures à la version 3.3.6r1 ;
  - Connectiva : toutes les versions de VNC antérieures à la version 3.3.3r2-21.
- Selon la distribution GNU/Linux, les versions vulnérables de TightVNC sont :
  - RedHat et Mandrake : toutes les versions de TightVNC antérieures à la version 1.2.5 ;
  - Gentoo : toutes les versions de TightVNC antérieures à la version 1.2.8 ;
  - Connectiva : toutes les versions de TightVNC antérieures à la version 1.2.6.

3 Résumé

Une vulnérabilité dans le serveur VNC (et TightVNC) permet à un utilisateur mal intentionné de se connecter au serveur VNC (et TightVNC) et ainsi avoir le contrôle à distance de la machine.

4 Description

VNC (Virtual Network Computing) est un logiciel de prise de contrôle à distance d'un ordinateur. TightVNC est une version dérivée de VNC permettant également le contrôle à distance de l'ordinateur et compatible avec ce dernier. Une vulnérabilté dans la création du cookie d'authentification au serveur X permet à un utilisateur mal intentionné de deviner le cookie d'authentification et de se connecter au serveur VNC ou TightVNC pour prendre le contrôle à distance de l'ordinateur.

5 Solution

Mettre à jour VNC et TightVNC en fonction de la distribution :

- Pour RedHat et Mandrake, mettre à jour VNC en version 3.3.3r2 et TightVNC en version 1.2.5 ;
- pour Gentoo, mettre à jour VNC en version 3.3.6r1 et TightVNC en version 1.2.8.
- pour Connectiva, mettre à jour VNC en version 3.3.3r2 et TightVNC en version 1.2.6.

6 Documentation

- Avis de sécurité RedHat RHSA-2003:041-12 :
  https://rhn.redhat.com/errata/RHSA-2003-041.html
- Avis de sécurité Mandrake MDKSA-2003:022 :
  http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2003:022
- Avis de sécurité Connectiva CLA-2003:640 :
  http://distro.conectiva.com.br/atualizacoes/?id=a&anuncio=000640
- Référence CVE CAN-2002-1336 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-1336
- Référence CVE CAN-2002-1511 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-1511

Gestion détaillée du document

28 février 2003 version initiale.
12 mai 2003 ajout des références CVE et du bulletin de sécurité de connectiva.