



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 15 novembre 2002
N° CERTA-2002-AVI-244-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de `lprng` et `html2ps` sous Linux

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-244>

Gestion du document

Référence	CERTA-2002-AVI-244-001
Titre	Vulnérabilité de <code>lprng</code> et <code>html2ps</code> sous Linux
Date de la première version	08 novembre 2002
Date de la dernière version	15 novembre 2002
Source(s)	Bulletin de sécurité SuSE-SA:2002:040 de SuSE
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

- Elévation de privilèges ;
- exécution de code arbitraire en local.

2 Systèmes affectés

- SuSE eMail server III, 3.1 ;
- SuSE Firewall on CD/admin host ;
- SuSE Firewall on CD 2 ;
- SuSE Linux Connectivity Server ;
- SuSE Linux Enterprise Server 7 ;
- SuSE Linux Office Server ;
- Linux Debian 3.0 (Woody) ;
- Linux Debain 2.2 (Potato) ;
- Linux Debian sid.

Il n'est cependant pas impossible que d'autres distributions de Linux soient affectées.

3 Résumé

Un utilisateur local peut exécuter des commandes avec les privilèges de l'administrateur `root` en passant certains paramètres à la commande `lpr`.

4 Description

LPRng est un module d'impression équivalent à `lpd` de plus en plus présent dans la plupart des distributions Unix ou Linux.

Ce paquetage contient un programme nommé `runlpr` permettant à l'utilisateur `lp` d'exécuter le programme `lpr` avec les privilèges de l'utilisateur `root`.

Un utilisateur local mal intentionné peut passer certains arguments à la ligne de commande `lpr` exécutée en tant que `root` de façon à exécuter du code arbitraire.

Les filtres d'impression de l'outil `html2ps` permettent aussi d'utiliser cette vulnérabilité.

Nota : Il faut avoir compromis le compte `lp` pour exploiter cette vulnérabilité.

5 Contournement provisoire

Désinstaller `html2ps` et `lprng` s'ils ne sont pas utilisés.

6 Solution

Se référer aux bulletins de sécurité et d'alerte (voir le paragraphe Documentation) des éditeurs pour connaître la disponibilité des correctifs.

7 Documentation

- Bulletin de sécurité SuSE-SA:2002:040 de SuSE :
http://www.suse.com/de/security/2002_040_lprng_html2ps.html
- Bulletin de sécurité DSA-192-1 de Debian :
<http://www.debian.org/security/2002/dsa-192>

Gestion détaillée du document

08 novembre 2002 version initiale.

15 novembre 2002 première révision : ajout du bulletin de sécurité de Debian.