Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 6 novembre 2002
N° CERTA-2002-AVI-235-003

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité des services `ypserv` et `ypxfrd` sous Unix

Gestion du document

Référence	CERTA-2002-AVI-235-003
Titre	Vulnérabilité des services `ypserv` et `ypxfrd` sous Unix
Date de la première version	17 octobre 2002
Date de la dernière version	6 novembre 2002
Source(s)	Bulletin de sécurité de IBM Bulletin de sécurité #SRB0051W de Compaq Bulletin d'alerte de Sun #473417 Note de vulnérabilité du CERT/CC VU#538033 Bulletin de sécurité #DSA-180-1 de Debian Bulletin de sécurité RHSA-2002:23-07 de RedHat
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

Accès en lecture à des données non autorisées.

2 Systèmes affectés

- Les systèmes AIX 4.3.x et 5.1.x d'IBM ;
- les systèmes HP-UX suivants :
  - HP-UX 10.20 ;
  - HP-UX 11.0 ;
  - HP-UX 11.11 ;
  - HP-UX 11.22 ;

- les systèmes HP Tru64 suivants :
  - Tru64 Unix 5.1A ;
  - Tru64 Unix 5.1 ;
  - Tru64 Unix 5.0A ;
  - Tru64 Unix 4.0G ;
  - Tru64 Unix 4.0F.
- les versions suivantes de Solaris pour Sparc et pour Intel :
  - Solaris 2.5.1 ;
  - Solaris 2.6 ;
  - Solaris 7 ;
  - Solaris 8 ;
  - Solaris 9 ;
- Debian Gnu/Linux 2.2 (Potato) et 3.0 (Woody).
- Il n'est cependant pas impossible que d'autres systèmes Unix ou Linux soient affectés.

3 Résumé

Un utilisateur local peut, en utilisant une vulnérabilité des services `ypserv` et `ypxfrd`, lire des fichiers auxquels il n'a normalement pas accès.

4 Description

NIS (Network Information Service) est un service sous Unix permettant de centraliser les informations relatives aux comptes des utilisateurs du réseau.

`ypserv` est le serveur permettant de rechercher des informations dans la base de données regroupant ces informations.

`ypxfrd` est un outil permettant de faire des transferts de bases de données (appelées `map`).

Un utilisateur local mal intentionné peut, au moyen de liens symboliques (astucieusement construits), amener les *daemons* `ypserv` et `ypxfrd` d'un serveur NIS à donner l'accès en lecture à des fichiers auxquels il n'aurait normalement pas accès.

5 Contournement provisoire

- En attendant l'application des correctifs, désactiver les *daemons* `ypserv` et `ypxfrd` si cela est possible.
- Supprimer les *daemons* `ypserv` et `ypxfrd` des systèmes sur lesquels ils ne sont pas utilisés.
- Limiter les machines autorisées à utiliser les services NIS (utiliser `/var/yp/securenets sous AIX`).

6 Solution

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

7 Documentation

- Bulletin de sécurité d'IBM :
  http://www-1.ibm.com/services/continuity/recover1.nsf/MSS/MSS-OAR-E01-2002.836.1
- Bulletin de sécurité #SRB0051W de Compaq :
  http://wwss1pro.compaq.com/support/reference_library/viewdocument.asp?source=SRB0051W.xml&dt=11

- Bulletin d'alerte #473417 de SUN :
  http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F47903
- Note de vulnérabilité VU#538033 du CERT/CC :
  http://www.kb.cert.org/vuls/id/538033
- Bulletin de sécurité #DSA-180-1 de Debian :
  http://www.debian.org/security/2002/dsa-180
- Bulletin de sécurité RHSA-2002:223-07 de RedHat :
  http://rhn.redhat.com/errata/RHSA-2002-223.html

Gestion détaillée du document

17 octobre 2002 version initiale.
21 octobre 2002 première révision : ajout des bulletins de sécurité IBM et HP ;
24 octobre 2002 seconde révision : ajout du bulletin de sécurité Debian ;
6 novembre 2002 troisième révision : ajout du bulletin de sécurité RedHat.