Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 08 octobre 2001
N° CERTA-2001-AVI-112-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de yppasswd

Gestion du document

Référence	CERTA-2001-AVI-112-001
Titre	Vulnérabilité de yppasswd
Date de la première version	08 octobre 2001
Date de la dernière version	08 octobre 2001
Source(s)	Bulletin d'alerte SUN numéro 27486 Note de Vulnérabilité du CERT/CC
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 à distance.

2 Systèmes affectés

Tous les serveurs NIS sous Solaris 2.6, 7 ou 8 et dont le *daemon* `rpc.yppasswdd` est en fonction.

3 Résumé

Un débordement de mémoire du *daemon* `rpc.yppasswdd` permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance.

4 Description

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

`yppasswd` permet aux utilisateurs de changer leur mot de passe.

Un utilisateur distant mal intentionné peut exécuter du code arbitraire au moyen d'un débordement de mémoire du *daemon* `rpc.yppasswdd`.

Cette attaque arrête le *daemon* `rpc.yppasswdd` ce qui empêche, par conséquent, les utilisateurs de changer de mot de passe.

5 Contournement provisoire

Arrêter le *daemon* `rpc.yppasswdd`. Ceci aura pour conséquence d'empêcher les utilisateurs de changer de mot de passe.

6 Solution

Télécharger et appliquer le correctif selon le système :

- Solaris 2.6 pour SPARC : 106303-03
- Solaris 7 pour SPARC : 111590-02
- Solaris 8 pour SPARC : 111596-02
- Solaris 2.6 pour architecture x86 : 106304-03
- Solaris 7 pour architecture x86 : 111591-02
- Solaris 8 pour architecture x86 : 111597-02

http://www.sunsolve.sun.com

7 Documentation

- Bulletin d'alerte de SUN numéro 27486 :
  http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=salert%2F27486
- Avis de Vulnérabilité VU#327281 du CERT/CC :
  http://www.kb.cert.org/vuls/id/327281

Gestion détaillée du document

08 octobre 2001 version initiale.

08 octobre 2001 seconde version : Inversion des correctifs SPARC et x386 dans le paragraphe solution.