Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 20 décembre 2002
N° CERTA-2001-AVI-045-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Débordement de mémoire dans NTPd

Gestion du document

Référence	CERTA-2001-AVI-045-002
Titre	Débordement de mémoire dans NTPd
Date de la première version	20 avril 2001
Date de la dernière version	20 décembre 2002
Source(s)	Avis de sécurité Linux Debian, Mandrake, 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

Exécution de code arbitraire à distance.

2 Systèmes affectés

Toute machine Unix équipée du service NTP (*Network Time Protocol*) dont le numéro de version est inférieur ou égal à 4.0.99k.

Nota : Les équipement CISCO sous IOS et possédant un serveur NTP sont vulnérables.

3 Résumé

Un utilisateur mal intentionné peut exécuter à distance du code arbitraire sur un serveur NTP. Ce code sera exécuté avec les privilèges de l'administrateur *root* dans la plupart des cas.

4 Description

Il est possible à un utilisateur mal intentionné d'effectuer un débordement de mémoire du *daemon* `ntpd` lorsque ce dernier doit répondre à une requête de dimension trop importante.

L'exploitation de cette vulnérabilité permet d'exécuter du code arbitraire à distance avec les droits du *daemon* `ntpd` (généralement *root*).

5 Contournement provisoire

Bloquer l'accès au service `NTP` (port 123 en UDP) à l'aide du garde barrière, ou en limiter les accès à votre serveur `NTP` uniquement aux clients autorisés.

Le bulletin de sécurité CISCO (voir paragraphe documentation) explique comment empêcher le traitement des requêtes `NTP`, employer l'authentification sur le protocole `NTP` ou bien ajouter des `ACL` (*Access Control Lists*) sous IOS.

6 Solution

Se référer aux bulletins de sécurité (voir paragraphe documentation) des différentes distributions ou contacter le distributeur pour connaitre la disponibilité des correctifs.

7 Documentation

- Bulletin de sécurité Hewlett Packard pour HP-UX 10.20, 10.24, 11.0, 11.04 et 11.11 :
  http://archives.neohapsis.com/archives/hp/2002-q4/0061.html
- Bulletin de sécurité CISCO :
  http://www.cisco.com/warp/public/707/NTP-pub.shtml
- Avis de sécurité Debian :
  http://www.debian.org/security/2001/dsa-045
- Avis de sécurité RedHat :
  http://www.redhat.com/support/errata/RHSA-2001-045.html
- Avis de sécurité Mandrake :
  http://www.linux-mandrake.com/en/security/2001/MDKSA-2001-036.php3?dis=7.2

Gestion détaillée du document

20 avril 2001 version initiale.

13 mai 2002 seconde version : ajout de CISCO, et relativisation des liens dans le paragraphe Solution.

20 décembre 2002 troisième version : ajout du constructeur HP.