Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 11 juin 2009
N° CERTA-2009-AVI-195-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans ntpd

Gestion du document

Référence	CERTA-2009-AVI-195-001
Titre	Vulnérabilités dans ntpd
Date de la première version	19 mai 2009
Date de la dernière version	11 juin 2009
Source(s)	Bulletin de sécurité Red Hat RHSA-2009-1039 du 18 mai 2009
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 ;
- déni de service à distance ;
- contournement de la politique de sécurité.

2 Systèmes affectés

Les versions de ntp antérieures à 4.2.4p7.

3 Résumé

Des vulnérabilités ont été identifiées dans le démon en charge de la maintenance et la synchronisation de l'heure ntpd. Elles peuvent être exploitées à distance par le biais de trames spécialement construites afin de perturber le service, voire d'exécuter du code arbitraire.

4 Description

Des vulnérabilités ont été identifiées dans le démon en charge de la maintenance et la synchronisation de l'heure ntpd.

- l'une d'elles fonctionne lorsque l'authentification NTP est activée (support OpenSSL). Des requêtes spécialement construites peuvent être incorrectement manipulées par la fonction `crypto_rcv()` de ntpd/ntp_crypto.c lorsque l'option `autokey` est utilisée (cette option est visible dans le fichier de configuration ntp.conf avec la présence de la ligne contenant "crypto pw XXX") ;
- des réponses provoquées par l'utilisation de la commande de diagnostic ntpq ne seraient pas correctement manipulées.

Ces vulnérabilités peuvent être exploitées à distance par le biais de trames spécialement construites afin de perturber le service, voire d'exécuter du code arbitraire.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité RedHat RHSA-2009:1039 du 18 mai 2009 :
  http://rhn.redhat.com/errata/RHSA-2009-1039.html
- Bulletin de sécurité RedHat RHSA-2009:1040 du 18 mai 2009 :
  http://rhn.redhat.com/errata/RHSA-2009-1040.html
- Note de vulnérabilité de l'US-CERT VU#853097 du 18 mai 2009 :
  http://www.kb.cert.org/vuls/id/853097
- Bulletin de sécurité FreeBSD SA-09:09.ntpd du 10 juin 2009 :
  http://security.freebsd.org/advisories/FreeBSD-SA-09:09.ntpd.asc
- Référence CVE CVE-2009-1252 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1252
- Référence CVE CVE-2009-0159 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0159
- Site officiel de téléchargement du projet ntp :
  http://www.ntp.org/downloads.html
- Site présentant l'outil de diagnostic ntpq associé à ntpd :
  http://www.cis.undel.edu/ mills/ntp/html/ntpq.html

Gestion détaillée du document

19 mai 2009 version initiale.
11 juin 2009 ajout du bulletin de sécurité FreeBSD.