Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 26 mai 2006
N° CERTA-2006-AVI-218

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Tor

Gestion du document

Référence	CERTA-2006-AVI-218
Titre	Multiples vulnérabilités dans Tor
Date de la première version	26 mai 2006
Date de la dernière version	–
Source(s)	Bulletin de mise à jour Tor du 23 mai 2006
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

- Déni de service ;
- contournement de la politique de sécurité ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

Toutes les versions de Tor antérieures à 0.1.1.20.

3 Résumé

Plusieurs vulnérabilités ont été identifiées dans Tor. Elles peuvent permettre à un utilisateur d'effectuer des actions malveillantes, comme la modification du processus de journalisation, un déni de service, ou encore la récupéreration d'informations sensibles.

4 Description

Tor est un réseau de tunnels virtuels permettant de garantir une certaine anonymité au cours de la navigation sur Internet. Chaque utilisateur participe à sa construction. Plusieurs vulnérabilités ont été identifiées dans les versions de Tor antérieures à 0.1.1.20. Parmi celles-ci :

- les chaînes de caractères venant du réseau ne sont pas correctement vérifiées. Un utilisateur malveillant peut altérer l'intégrité des journaux avant qu'ils ne soient affichés.
- les options de pare-feu ne sont pas scrupuleusement respectées. La politique de sécurité peut alors être contournée.
- des attaques de type débordement de mémoire sont possibles quand des éléments sont ajoutés dans la liste courante (ou *smartlist*).
- les clés de chiffrement ne sont pas renouvelées lorsque l'utilisateur change son adresse IP.
- il est possible de deviner le choix des noeuds internes à partir d'attaques statistiques, connaissant les chemins (ou *circuits*) ayant des noeuds de sortie.
- il n'est pas possible de choisir, voire d'imposer, une liste de noeuds d'entrée. Ceci favorise alors les attaques de proximité issues de noeuds inconnus.

5 Solution

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

6 Documentation

- Référence CVE CVE-2006-0414 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0414
- Mise à jour de Tor :
  http://tor.eff.org/download.html.fr
- Détails sur la mise à jour de sécurité de la version 1.1.20 de Tor :
  http://tor.eff.org/cvs/tor/ChangeLog

Gestion détaillée du document

26 mai 2006 version initiale.