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 juin 2008
N° CERTA-2008-AVI-340

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Cisco VPN Client

Gestion du document

Référence	CERTA-2008-AVI-340
Titre	Vulnérabilité dans Cisco VPN Client
Date de la première version	26 juin 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco CSCsm25860
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

Élévation de privilèges.

2 Systèmes affectés

- Cisco VPN Client 2.x ;
- Cisco VPN Client 3.x ;
- Cisco VPN Client 4.x ;
- Cisco VPN Client 5.x.

D'autres produits sont affectés par la même vulnérabilité (BlueCoat Winproxy, produits SafeNet).

3 Résumé

Une vulnérabilité dans *Cisco VPN Client* permet à une personne malintentionnée locale d'élever ses privilèges.

4 Description

Une vulnérabilité a été découverte dans *Cisco VPN Client* dans le pilote *Deterministic Network Enhancer* `dne2000.sys`. Cette faille peut être exploitée par une personne malintentionnée locale pour exécuter du code arbitraire avec des privilèges système.

Les versions du pilote qui sont affectées sont 2.21.7.233 à 3.21.7.17464.

5 Solution

Mettre à jour Cisco VPN Client à la version 5.0.03.0530. La version 3.21.12.17902 du pilote DNE corrige également le problème.

6 Documentation

- Bulletin de sécurité Cisco CSCsm25860 :
  http://tools.cisco.com/Support/BugToolkit/search/getBugDetails.do?method=fetchBugDetails&bugId=CSCsm25860

- Mise à jour du pilote DNE :
  http://www.deterministicnetworks.com/support/dnesupport.asp
- Note de vulnérabilité de l'US-CERT VU#858993 du 18 juin 2008 :
  http://www.kb.cert.org/vuls/id/858993

Gestion détaillée du document

26 juin 2008 version initiale.