Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 02 novembre 2007
N° CERTA-2007-AVI-472

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités de SonicWALL SSL VPN

Gestion du document

Référence	CERTA-2007-AVI-472
Titre	Multiples vulnérabilités de SonicWALL SSL VPN
Date de la première version	02 novembre 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité US-CERT VU#298521 du 01 novembre 2007
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 ;
- contournement de la politique de sécurité ;
- atteinte à l'intégrité des données.

2 Systèmes affectés

- SonicWALL SSL-VPN 200 versions antérieures à la version 2.1 ;
- SonicWALL SSL-VPN 2000 versions antérieures à la version 2.5 ;
- SonicWALL SSL-VPN 4000 versions antérieures à la version 2.5.

3 Résumé

Plusieurs vulnérabilités ont été découvertes dans SonicWALL SSL-VPN. Ces vulnérabilités peuvent être exploitées afin de porter atteinte à l'intégrité du système ou d'exécuter du code arbitraire à distance.

4 Description

Deux vulnérabilités ont été découvertes dans `SonicWALL SSL-VPN:`

- Une erreur aux limites a été découverte dans le contrôle ActiveX *NetExtender NELaunchCtrl*. Cette vulnérabilité peut être exploitée via un site malicieux, exécutant ainsi du code arbitraire sur le poste de l'utilisateur.
- L'utilisation de la méthode *FileDelete()* dans le contrôle ActiveX *WebCacheCleaner* peut être exploitée afin d'effacer des fichiers arbitraires.

5 Solution

Installer la version de *firmware* 2.1 pour les SonicWALL SSL-VPN 200 et la version 2.5 pour les SonicWALL SSL-VPN 2000 et 4000 (cf. documentation pour l'adresse de téléchargement).

6 Documentation

- Téléchargement des mises à jour sur le site de l'éditeur :
  http://www.sonicwall.com/us/643.htm
- Note de vulnérabilité de l'US-CERT VU#298521 du 01 novembre 2007 :
  http://www.kb.cert.org/vuls/id/298521
- Référence CVE CVE-2007-5603 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5603

Gestion détaillée du document

02 novembre 2007 version initiale.