

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans SonicWALL SSL-VPN

---

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>  
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2009-AVI-226>

---

### Gestion du document

Référence	CERTA-2009-AVI-226
Titre	Vulnérabilité dans SonicWALL SSL-VPN
Date de la première version	10 juin 2009
Date de la dernière version	–
Source(s)	Note de mise à jour SonicWALL pour les versions 3.0.0.9 et 3.5.0.5
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 ;
- atteinte à la confidentialité des données.

## 2 Systèmes affectés

- SonicWALL SSL-VPN 200 versions antérieures à la version 3.0.0.9 ;
- SonicWALL SSL-VPN 2000 versions antérieures à la version 3.5.0.5 ;
- SonicWALL SSL-VPN 4000 versions antérieures à la version 3.5.0.5.

## 3 Résumé

Une vulnérabilité permettant de réaliser, entre autre, une exécution de code arbitraire à distance a été découverte dans SonicWALL SSL-VPN.

## **4 Description**

Une vulnérabilité a été découverte dans SonicWALL SSL-VPN. Cette vulnérabilité est due à une erreur dans le traitement des chaînes de format. L'exploitation de cette vulnérabilité permet à une personne distante malintentionnée de récupérer des données sensibles, de réaliser un déni de service ou 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**

- Site de l'éditeur permettant d'obtenir les mises à jour de micrologiciel (*firmware*):  
<http://www.mysonicwall.com>

## **Gestion détaillée du document**

**10 juin 2009** version initiale.