

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du produit SonicWALL

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-2008-AVI-539>

Gestion du document

| | |
|-----------------------------|--|
| Référence | CERTA-2008-AVI-539 |
| Titre | Vulnérabilité du produit SonicWALL |
| Date de la première version | 05 novembre 2008 |
| Date de la dernière version | – |
| Source(s) | Note de mise à jour SonicWALL pour le passage à la version 4.0.1.1 |
| 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

Injection de code indirecte (*Cross Site Scripting*)

2 Systèmes affectés

Produits SonicWALL fonctionnant sous le système SonicWALL dans une version antérieure à la version 4.0.1.1 (SonicWALL Pro Series et SonicWALL TZ Series).

3 Résumé

Une vulnérabilité permettant de conduire des attaques par injection de code indirecte a été découverte dans certains produits SonicWALL.

4 Description

Une vulnérabilité a été découverte dans la manière de gérer les variables des URL par certains produits SonicWALL. Cette vulnérabilité peut être exploitée afin de conduire une attaque par injection de code indirecte.

5 Solution

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

6 Documentation

- Annonce de la version 4.0.1.1 de SonicWALL :
http://www.sonicwall.com/downloads/SonicOS_Enhanced_4.0.1.1_Release_Notes.pdf

Gestion détaillée du document

05 novembre 2008 version initiale.