Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 21 août 2007
N° CERTA-2007-AVI-370

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans les produits ZoneLabs

Gestion du document

Référence	CERTA-2007-AVI-370
Titre	Vulnérabilités dans les produits ZoneLabs
Date de la première version	21 août 2007
Date de la dernière version	–
Source(s)	Bulletins de sécurité iDefense du 20 août 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

Élévation de privilèges.

2 Systèmes affectés

- *ZoneAlarm* versions 2.x, 3.x, 4.x, 5.x, 6.x, 7.x ;
- *ZoneAlarm Plus* versions 3.x, 4.x ;
- *ZoneAlarm Pro* versions 2.x, 3.x, 4.x, 5.x, 6.x ;
- *ZoneAlarm Anti-Spyware* versions 6.x ;
- *ZoneAlarm Antivirus* versions 5.x, 6.x ;
- *ZoneAlarm Internet Security Suite* versions 6.x ;
- *ZoneAlarm Security Suite* versions 5.x ;
- *ZoneAlarm Wireless Security* versions 5.x.

3 Résumé

Deux vulnérabilités dans les produits *ZoneLabs* permettent une élévation de privilèges.

4 Description

Deux vulnérabilités ont été découvertes dans les produits *ZoneLabs*.

Lorsqu'un administrateur installe un produit *ZoneLabs* de la famille *ZoneAlarm*, un paramétrage par défaut permet à tout utilisateur de modifier les fichiers installés (référence CVE-2005-2932). Certains de ces fichiers sont exécutés avec les droits `system`.

Une vulnérabilité a été découverte dans le pilote `vsdatant.sys`. Cette vulnérabilité permet à un utilisateur local de modifier directement le contenu de certaines zones de la mémoire (référence CVE-2007-4216).

5 Solution

Mettre à jour en version 7.0.362 (cf. section Documentation).

6 Documentation

- Page de mise à jour de ZoneAlarm :
  http://www.zonealarm.com/store/content/support/zasc/cfu.jsp?dc=12bms&ctry=FR&lang=fr&lid=db_updates
- Bulletins de sécurité iDefense du 20 août 2007 :
  http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=584
  http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=585
- Référence CVE-2005-2932 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-2932
- Référence CVE-2007-4216 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4216

Gestion détaillée du document

21 août 2007 version initiale.