

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans plusieurs antivirus

---

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-2004-AVI-349>

---

### Gestion du document

Référence	CERTA-2004-AVI-349
Titre	Vulnérabilité dans plusieurs antivirus
Date de la première version	21 octobre 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité iDefense 10.18.04
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

- Contournement de la protection antivirale.

## 2 Systèmes affectés

Plusieurs antivirus sont affectés par cette vulnérabilité :

- eTrsut antivirus
- Kaspersky antivirus ;
- Sophos antivirus ;
- McAfee ;
- NOD32 ;
- RAV antivirus.

Pour plus de détails sur les versions des systèmes affectées, se référer au bulletin de sécurité de l'éditeur (cf. section Documentation).

## 3 Résumé

Une vulnérabilité présente lors du traitement des fichiers au format zip par les antivirus permet à un utilisateur mal intentionné de contourner la protection apportée par ces antivirus.

## 4 Description

L'information sur les fichiers compressés à l'intérieur d'un fichier au format zip est stockée dans un en-tête local (créé avant la compression de chaque fichier) et un en-tête global (créé après la compression de tous les fichiers).

Un utilisateur mal intentionné peut changer la taille des fichiers à l'intérieur des entêtes local et global afin de contourner la protection antivirale apportée par l'antivirus.

## 5 Contournement provisoire

Filtrer les messages contenant une pièce jointe au format zip.

## 6 Solution

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

Pour l'antivirus NOD32 la vulnérabilité a été corrigée dans la version 1.020 du module archive-support disponible lors de la mise à jour des signatures de virus.

## 7 Documentation

- Bulletin de sécurité de iDefense du 18 octobre 2004 :  
<http://www.iddefense.com/application/poi/display?id=153&type=vulnerabilities>
- Bulletin de sécurité Sophos du 19 octobre 2004 :  
<http://sophos.com/support/knowledgebase/article/2074.html>
- Bulletin de sécurité McAfee (Utilisateur) :  
<http://download.mcafee.com/uk/updates/updates.asp>
- Bulletin de sécurité McAfee (Entreprise) :  
<http://www.mcafeesecurity.com/uk/downloads/updates/dat.asp?id=1>
- Bulletin de sécurité Computer Associates :  
[http://supportconnectw.ca.com/public/ca\\_common\\_docs/arclib\\_vuln.asp](http://supportconnectw.ca.com/public/ca_common_docs/arclib_vuln.asp)
- Référence CVE CAN-2004-0937 concernant la vulnérabilité sur Sophos antivirus :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0937>
- Référence CVE CAN-2004-0936 concernant la vulnérabilité sur RAV antivirus :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0936>
- Référence CVE CAN-2004-0935 concernant la vulnérabilité sur NOD32 antivirus :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0935>
- Référence CVE CAN-2004-0934 concernant la vulnérabilité sur Kaspersky antivirus :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0934>
- Référence CVE CAN-2004-0933 concernant la vulnérabilité sur eTrust de Computer Associates :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0933>
- Référence CVE CAN-2004-0932 concernant la vulnérabilité sur McAfee antivirus :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0932>

## Gestion détaillée du document

21 octobre 2004 version initiale.