

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité d'un grand nombre d'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-2005-ALE-014>

Gestion du document

| | |
|-----------------------------|---|
| Référence | CERTA-2005-ALE-014 |
| Titre | Vulnérabilité d'un grand nombre d'antivirus |
| Date de la première version | 11 octobre 2005 |
| Date de la dernière version | – |
| Source(s) | Bulletin de "Security Focus" |
| 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 politique de sécurité ;
- contournement du système de filtrage de l'antivirus.

2 Systèmes affectés

La majorité des antivirus du marché ont été recensés comme vulnérables. Sont concernés :

- VirusBlokAda VBA32
- Ukrainian Antiviral Center Ukrainian National Antivirus
- Symantec Norton Antivirus
- Sophos Anti-Virus
- Softwin BitDefender
- Panda Antivirus
- Panda ActiveScan
- Norman Virus Control
- McAfee VirusScan
- Kaspersky Labs (tous produits)
- Ikarus

- Hacksoft TheHacker
- H+BEDV AntiVir
- Fortinet Antivirus
- F-Secure Anti-Virus
- Eset Software NOD32 Antivirus
- Dr.Web
- Computer Associates Vet Antivirus
- Computer Associates eTrust EZ Antivirus
- Clam Anti-Virus ClamAV
- Cat Computer Services Quick Heal Antivirus
- AVG AVG Anti-Virus
- Avast! Antivirus
- ArcaBit ArcaVir

Pour obtenir la liste détaillée des versions vulnérables, se reporter au bulletin de Security Focus (cf. Documentation).

3 Résumé

Une vulnérabilité dans le traitement des archives affecte la quasi-totalité des antivirus du marché. Ainsi, les antivirus ne peuvent repérer un virus inséré dans une archive malicieusement construite.

4 Description

La plupart des antivirus du marché sont vulnérables à un contournement de politique de sécurité.

En effet, il est possible grâce à un fichier archive malicieusement construit, de passer outre le système de filtrage de l'antivirus. Ainsi, un virus contenu dans ce fichier archive sera acheminé vers son destinataire sans traitement préalable par une passerelle antivirus.

Une fois arrivé sur le poste utilisateur, le fichier virus contenu dans l'archive doit être extrait puis exécuté par l'utilisateur pour corrompre la machine.

5 Contournement provisoire

Tant que le virus n'est pas extrait de l'archive sur le poste client cible, aucun code malveillant n'est exécuté. Il convient donc de respecter les règles de comportement élémentaires d'utilisation de la messagerie, rappelés ci-dessous :

- mettre à jour son antivirus ;
- ne pas ouvrir les mails à caractère douteux ;
- ne jamais ouvrir les fichiers archives en cas de doute sur leur provenance ;
- vérifier systématiquement le contenu extrait des archives ;
- Dans le cadre de la défense en profondeur, privilégier systématiquement l'emploi d'un antivirus sur la passerelle de messagerie associé à un antivirus différent sur les postes de travail.

6 Solution

Aucune solution n'a été communiquée pour l'instant par les éditeurs d'antivirus.

7 Documentation

- Bulletin de Security Focus :
<http://www.securityfocus.com/bid/15046>
- Mémento du CERTA sur les virus : CERTA-2005-MEM-001
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-MEM-001.pdf>

Gestion détaillée du document

11 octobre 2005 version initiale.