

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans plusieurs produits de Computer Associates

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-AVI-176>

Gestion du document

Référence	CERTA-2005-AVI-176
Titre	Vulnérabilité dans plusieurs produits de Computer Associates
Date de la première version	25 mai 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité #32896 du 24 mai 2005
Pièce(s) jointe(s)	

TAB. 1 – Gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

Exécution de code arbitraire.

2 Systèmes affectés

- eTrust Secure Content Manager 1.0, 1.0 SP1 & 1.1 ;
- eTrust Intrusion Detection 1.4.1.13, 2.0, 2.0 SP1, 3.0 & 3.0 SP1 ;
- eTrust EZ Antivirus version 6.1 à la version 7.0.5 ;
- eTrust EZ Armor version 1.0 à la version 3.1 ;
- eTrust EZ Armor LE version 2.0 à la version 3.0.0.14 ;
- CA InoculateIT 6.0 ;
- Vet Antivirus 10.66 et versions antérieures ;
- BrightStor ARCserve Backup r11.1 pour Windows.

Tous les systèmes d'exploitation, ainsi que Lotus Notes/Exchange sont concernés par la vulnérabilité affectant les produits suivants :

- eTrust Antivirus r6.0 ;
- eTrust Antivirus r7.0 ;

- eTrust Antivirus r7.1 ;
- eTrust Antivirus for the Gateway r7.0 ;
- eTrust Antivirus for the Gateway r7.1.

3 Résumé

Une vulnérabilité présente dans de nombreux produits de Computer Associates permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance.

4 Description

Plusieurs produits de Computer Associates sont touchés par une vulnérabilité affectant la bibliothèque de liaison dynamique (`Dynamic Link Library`) *Vet Antivirus Engine VetE.dll*. Cette vulnérabilité de type débordement de mémoire permet à un utilisateur distant mal intentionné d'exécuter du code arbitraire au moyen de paquets malicieusement contruits basés sur des protocoles courants (SMTP, FTP, SMB etc.).

5 Solution

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

6 Documentation

- Bulletin de sécurité Computer Associates #32896 du 24 mai 2005 :
<http://www3.ca.com/securityadvisor/vulninfo/vuln.aspx?id=32896>
- Référence CVE CAN-2005-1693 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1693>

Gestion détaillée du document

25 mai 2005 version initiale.