Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 09 février 2005
N° CERTA-2005-AVI-052

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités sur le traitement des objets OLE et COM

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-052

Gestion du document

Référence	CERTA-2005-AVI-052
Titre	Vulnérabilités sur le traitement des objets OLE et COM
Date de la première version	09 février 2005
Date de la dernière version	–
Source(s)	Bulletin de securite MS05-012
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

- Execution de code arbitraire ;
- élévation de privilèges.

2 Systèmes affectés

- Microsoft Windows 2000 Server ;
- Microsoft Windows 2000 Advanced Server ;
- Microsoft Windows 2000 Datacenter Server ;
- Microsoft Windows 2000 Professional ;
- Microsoft Windows 98 ;
- Microsoft Windows 98 seconde édition ;
- Microsoft Windows Millenium ;
- Microsoft Windows Server 2003 édition Datacenter ;
- Microsoft Windows Server 2003 édition entreprise ;
- Microsoft Windows Server 2003 édition standard ;
- Microsoft Windows Server 2003 édition web ;

3 Résumé

Deux vulnérabilités sont présentes dans le traitement des objets OLE et COM. Ces deux vulnérabilités peuvent être exploitées par un utilisateur local mal intentionné pour exécuter du code arbitraire avec des privilèges élevés.

4 Description

Deux vulnérabilités sont présentes dans le traitement de certains objets sur Microsoft Windows :

- La première vulnérabilité est présente dans le traitement des objets OLE. Un utilisateur mal intentionné peut, par le biais d'un logiciel utilisant les objets OLE, exploiter la vulnérabilité en envoyant un objet OLE malicieusement construit.
- La seonde vulnérabilité est présente dans le traitement des structures de données COM. Un utilisateur local mal intentionné peut exécuter du code arbitaire avec des accès privilègiés en exploitant cette vulnérabilité

Un grand nombre de logiciels sont également touchés par ces vulnérabilités car ils utilisent les objets COM du système d'exploitation.

5 Solution

Se référer aux bulletins de sécurité des éditeurs (cf. section Documentation) pour l'obtention des correctifs.

6 Documentation

- Bulletin de sécurité Microsoft MS05-012 du 8 février 2005 :
  http://www.microsoft.com/technet/security/bulletin/ms05-012.mspx
- Référence CVE CAN-2005-0047 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0047
- Référence CVE CAN-2005-0044 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0044

Gestion détaillée du document

09 février 2005 version initiale.