Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 16 août 2005
N° CERTA-2005-ALE-007

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Exploitation de la faille MS05-039 (*plug and play* sur des systèmes Microsoft)

Gestion du document

Référence	CERTA-2005-ALE-007
Titre	Exploitation de la faille MS05-039
Date de la première version	16 août 2005
Date de la dernière version	–
Source(s)	Avis CERTA-2005-AVI-302 Avis Microsoft MS05-039 Avis de sécurité Microsoft 899588
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

Exécution de code arbitraire.

2 Systèmes affectés

Voir avis CERTA-2005-AVI-302.

3 Description

Le savoir faire pour exploiter la vulnérabilité pour laquelle un correctif est décrit dans l'avis CERTA-2005-AVI-302 a été publié.

Ce savoir faire a été mis en œuvre sous la forme d'un ver appelé `Win32/Zotob.A` par certains éditeurs d'antivirus. Il est possible que d'autres formes d'exploitation de cette vulnérabilité apparaissent.

4 Contournement provisoire

Bien que ça ne puisse pas être généralisé à toutes les exploitations possibles de cette faille de sécurité, il se trouve que le ver `Win32/Zotob.A` :

- balaye le réseau pour y découvrir des machines vulnérables sur le port `445/TCP` ;
- essaye de se connecter à un serveur IRC ;
- génère du trafic sur les ports `8080/TCP`, `8888/TCP` et `33333/TCP`.

Une activité anormale sur ces ports peut aider l'administrateur du réseau à découvrir les machines contaminées par le ver.

5 Solution

Il est recommandé d'appliquer le correctif décrit dans l'avis CERTA-2005-AVI-302.

6 Documentation

- description de la vulnérabilité :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-AVI-302
- description du ver `Win32/Zotob.A` :
  http://www.microsoft.com/technet/security/advisory/899588.mspx

Gestion détaillée du document

16 août 2005 version initiale.