Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 11 février 2009
N° CERTA-2009-AVI-064

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans l'Autorun sur Windows

Gestion du document

Référence	CERTA-2009-AVI-064
Titre	Vulnérabilité dans l'Autorun sur Windows
Date de la première version	11 février 2009
Date de la dernière version	–
Source(s)	Alerte TA09-020A de l'US-CERT Bulletin Microsoft KB953252 du 05 février 2009
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 à distance ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- Microsoft Windows 2000 ;
- Microsoft Windows XP ;
- Microsoft Windows Server 2003.

3 Résumé

Une vulnérabilité dans Microsoft Windows permet le contournement de la politique de sécurité et l'exécution de code arbitraire à distance.

4 Description

Une vulnérabilité dans l'interprétation des paramètres d'autorun dans Microsoft Windows permet le contournement de la politique de sécurité et l'exécution de code arbitraire à distance. En effet, les paramètres définis par la valeur de la clé `NoDriveTypeAutorun` ne sont pas correctement interprétés par le système. L'exécution automatique de codes malveillants au travers de clés USB (via le menu contextuel, ou un double-clic sur l'icône) ou lecteurs réseau, par exemple, est donc possible sur des sytèmes vulnérables même si la clé de registre est supposée désactiver cette fonctionnalité.

La vulnérabilité a été corrigée pour les systèmes Windows Vista et Windows Server 2008 dans le correctif MS08-038, puis pour les autres systèmes Windows dans une mise à jour non automatique.

5 Solution

Cette mise à jour n'est pas disponible en mise à jour automatique. Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation). Remarque : le correctif porte la référence kb950582 alors que le bulletin porte la référence kb953252.

6 Documentation

- Bulletin de sécurité Microsoft KB953252 du 05 février 2009 :
  http://support.microsoft.com/kb/953252
- Note d'information « Risques associés aux clés USB » :
  http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-006/index.html
- Alerte de sécurité de l'US-CERT TA09-020A du 20 janvier 2009 :
  http://www.us-cert.gov/cas/techalerts/TA09-020A.html
- Référence CVE CVE-2008-0951 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0951

Gestion détaillée du document

11 février 2009 version initiale.