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 2011
N° CERTA-2011-AVI-068

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Kerberos dans Microsoft Windows

Gestion du document

Référence	CERTA-2011-AVI-068
Titre	Vulnérabilité de Kerberos dans Microsoft Windows
Date de la première version	09 février 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS11-013 du 08 février 2011
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

Élévation de privilèges.

2 Systèmes affectés

- Microsoft Windows XP service pack 3 ;
- Microsoft Windows XP x64 Edition service pack 2 ;
- Microsoft Windows 2003 service pack 2 ;
- Microsoft Windows 2003 x64 Edition service pack 2 ;
- Microsoft Windows 2003 service pack 2 pour les systèmes Itanium ;
- Windows 7 pour les systèmes 32-bit ;
- Windows 7 pour les systèmes x64 ;
- Windows Server 2008 R2 pour les systèmes x64 ;
- Windows Server 2008 R2 pour les systèmes Itanium.

3 Résumé

Une vulnérabilité dans la mise en œuvre de `Kerberos` sous `Microsoft Windows` permet à un utilisateur malintentionné d'élever ses privilèges.

4 Description

Une vulnérabilité est présente dans la mise en œuvre de `Kerberos` sous `Microsoft Windows`. Elle est due à la possibilité d'utiliser un algorithme de chiffrement obsolète lors de communications entre clients et serveur. La faiblesse du chiffrement peut alors permettre à un utilisateur malintentionné authentifié sur le domaine d'élever ses privilèges.

5 Solution

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

6 Documentation

- Bulletin de sécurité Microsoft MS11-013 du 08 février 2011 :
  http://www.microsoft.com/france/technet/security/Bulletin/MS11-013.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS11-013.mspx
- Référence CVE CVE-2011-0043 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0043
- Référence CVE CVE-2011-0091 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0091

Gestion détaillée du document

09 février 2011 version initiale.