Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 10 août 2005
N° CERTA-2005-AVI-302

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le module Plug and Play (PnP) de Windows

Gestion du document

Référence	CERTA-2005-AVI-302
Titre	Vulnérabilité dans le module Plug and Play (PnP) de Windows
Date de la première version	10 août 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité de Microsoft MS05-39 du 09 Août 2005
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 à distance ;
- élévation des privilèges locaux.

2 Systèmes affectés

- Microsoft Windows 2000 Service Pack 4 ;
- Microsoft Windows XP Service Pack 1 et Service Pack 2 ;
- Microsoft Windows XP Professional x64 Edition ;
- Microsoft Windows Server 2003 et Microsoft Windows Server 2003 Service Pack 1 ;
- Microsoft Windows Server 2003 et Microsoft Windows Server 2003 Service Pack 1 pour les systèmes basés sur Itanium ;
- Microsoft Windows Server 2003 x64 Edition.

3 Description

Une faille dans le module Plug and Play (PnP) de Microsoft Windows a été découverte. Elle permettrait à un utilisateur mal-intentionné de prendre le contrôle total du système vulnérable, à distance ou en local, par le biais d'une exécution de code malveillant.

Concernant Windows XP SP2 et Windows 2003, l'attaquant doit avant tout disposer d'un couple d'authentification valide et ne peut exploiter la vulnérabilité que localement.

Concernant Windows XP SP1, l'attaquant doit disposer d'un couple d'authentification valide.

4 Solution

Appliquer les correctifs de Microsoft.

5 Documentation

- Site de l'éditeur :
  http://www.microsoft.com
- Bulletin Microsoft du 09 Août 2005 :
  http://www.microsoft.com/technet/security/bulletin/MS05-039.mspx
- Référence CVE-CAN :
  http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1983

Gestion détaillée du document

10 août 2005 version initiale.