

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans la gestion d'IPv6 sous Windows

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-2006-AVI-444>

Gestion du document

Référence	CERTA-2006-AVI-444
Titre	Vulnérabilités dans la gestion d'IPv6 sous Windows
Date de la première version	11 octobre 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS06-064 du 10 octobre 2006
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

Déni de service à distance.

2 Systèmes affectés

- 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 (Itanium) et Microsoft Windows Server 2003 Service Pack 1 (Itanium) ;
- Microsoft Windows Server 2003 x64 Edition.

3 Résumé

Trois vulnérabilités affectant la mise en oeuvre d'IPv6 sous Windows permettent de réaliser des dénis de service à distance.

4 Description

Trois vulnérabilités affectant la mise en oeuvre d'IPv6 sous Windows ont été découvertes. Il s'agit d'anciennes vulnérabilités qui avaient fait l'objet d'un avis du CERTA (CERTA-2005-AVI-135) et qui avaient été corrigées par Microsoft pour IPv4 seulement (bulletin de sécurité MS05-019). Ces vulnérabilités permettent de mettre fin à une connexion TCP établie ou de l'ignorer (CVE-2004-0790 et CVE-2004-0230) et d'entraîner une consommation excessive des ressources CPU (CVE-2005-0688).

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 MS06-064 du 10 octobre 2006 :
<http://www.microsoft.com/technet/security/Bulletin/MS06-064.msp>
<http://www.microsoft.com/france/technet/security/Bulletin/MS06-064.msp>
- Bulletin de sécurité Microsoft MS05-019 du 12 avril 2005 :
<http://www.microsoft.com/technet/security/Bulletin/MS05-019.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS05-019.msp>
- Avis CERTA-2005-AVI-135 du 13 avril 2005 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-AVI-135/index.html>
- Référence CVE CVE-2004-0790 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-0790>
- Référence CVE CVE-2004-0230 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-0230>
- Référence CVE CVE-2005-0688 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-0688>

Gestion détaillée du document

11 octobre 2006 version initiale.