

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le service UPnP de Microsoft 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-2007-AVI-166>

Gestion du document

Référence	CERTA-2007-AVI-166
Titre	Vulnérabilité dans le service UPnP de Microsoft Windows
Date de la première version	11 avril 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS07-019 du 10 avril 2007
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.

2 Systèmes affectés

- Microsoft Windows XP Service Pack 2 ;
- Microsoft Windows XP Professional x64 Edition (Service Pack 2 compris).

3 Résumé

Une vulnérabilité a été identifiée dans le service *Universal Plug and Play* (UPnP) de Microsoft Windows. Une personne malveillante pourrait l'exploiter en envoyant un paquet spécialement construit vers le système vulnérable, et ainsi prendre le contrôle total de celui-ci.

4 Description

Une vulnérabilité a été identifiée dans le service *Universal Plug and Play* (UPnP) de Microsoft Windows. Ce service a pour but de faciliter la communication entre périphériques, et s'appuie fréquemment sur les protocoles

IP, TCP/UDP et HTTP. Outre une phase de découverte des services disponibles dans le réseau, il offre aussi la possibilité d'envoyer des actions et des notifications d'événements (mises à jour du service par exemple). Ce service est largement mise en œuvre, et se trouve bien souvent activé automatiquement dans les configurations par défaut des appareils. Il fait partie des exceptions autorisées par le pare-feu Windows dans son installation native.

Le système ne manipulerait pas correctement certaines requêtes HTTP. Une personne malveillante pourrait donc envoyer à distance un paquet spécialement construit vers le système vulnérable, et ainsi prendre le contrôle total de celui-ci.

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 MS07-019 du 10 avril 2007 :
<http://www.microsoft.com/france/technet/security/bulletin/MS07-019.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS07-019.msp>
- Bulletin de sécurité iDefense du 10 avril 2007 :
<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=509>
- Référence CVE CVE-2007-1204 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1204>
- Informations sur le service UPnP (Universal Plug and Play) :
<http://www.upnp.org>

Gestion détaillée du document

11 avril 2007 version initiale.