

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités du service d'authentification Internet de Microsoft

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-2009-AVI-537>

Gestion du document

Référence	CERTA-2009-AVI-537
Titre	Multiples vulnérabilités du service d'authentification Internet de Microsoft
Date de la première version	09 décembre 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft numéro MS09-071 du 08 décembre 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 ;
- élévation de privilèges.

2 Systèmes affectés

- Microsoft Windows 2000 Service Pack 4 ;
- Windows XP Service Pack 2 et Service Pack 3 ;
- Windows XP Pro édition x64 Service Pack 2 ;
- Windows Server 2003 toutes versions ;
- Windows Vista toutes versions ;
- Windows 2008 versions antérieures à la version R2.

3 Résumé

De multiples vulnérabilités ont été découvertes dans le service d'authentification Internet de Microsoft. L'exploitation de ces vulnérabilités permet entre autres d'exécuter du code arbitraire à distance.

4 Description

Deux vulnérabilités ont été découvertes dans le service d'authentification Internet de Microsoft :

- la première résulte d'une mauvaise implémentation du protocole d'authentification PAEP et permet l'exécution de code arbitraire à distance ;
- la seconde résulte d'une mauvaise gestion des requêtes d'authentification MS-CHAP v2 et permet à un utilisateur mal intentionné d'avoir accès à des ressources d'un utilisateur privilégié.

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 MS09-071 du 08 décembre 2009 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS09-071.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS09-071.msp>
- Référence CVE CVE-2009-2505 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2505>
- Référence CVE CVE-2009-3677 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3677>

Gestion détaillée du document

09 décembre 2009 version initiale.