

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans les services HTTP 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-2009-AVI-143>

Gestion du document

Référence	CERTA-2009-AVI-143
Titre	Vulnérabilités dans les services HTTP Windows
Date de la première version	15 avril 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS09-013 du 14 avril 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.

2 Systèmes affectés

- Microsoft Windows 2000 Service Pack 4 ;
- Microsoft Windows XP Service Pack 2 et 3 ;
- Microsoft Windows XP Professional Edition pour systèmes x64, Service Pack 2 compris ;
- Microsoft Windows Server 2003 Service Pack 1 et 2, y compris pour les systèmes x64 et Itanium ;
- Microsoft Windows Vista, Service Pack 1 inclus, y compris pour les versions x64 ;
- Microsoft Windows Server 2008 pour systèmes 32 bits, x64 et Itanium.

3 Résumé

Des vulnérabilités ont été identifiées dans les services HTTP Windows. L'exploitation de ces dernières à distance permet d'exécuter du code arbitraire sur le système vulnérable.

4 Description

Des vulnérabilités ont été identifiées dans les services HTTP Windows. Ces derniers (WinHTTP) fournissent des interfaces, ou API HTTP cliente pour communiquer en HTTP. Ces interfaces sont donc utilisées par les composants Windows (par exemple le service UPnP *Universal Plug-and-Play*) ou par des applications tiers.

Les interfaces ne valident pas correctement certains champs retournés dans les réponses par les serveurs. Elles peuvent aussi être exploitées dans le cas d'attaques par « réflexion » qui permettent de réutiliser les informations d'authentification Windows. Enfin, les certificats des sites Web ne sont validés qu'en fonction du nom de domaine complet de l'URL et WinHTTP peut cacher les incohérences de validation à l'utilisateur.

Ces vulnérabilités peuvent être exploitées à distance afin d'exécuter du code arbitraire sur le système vulnérable.

5 Solution

Se référer au bulletin de sécurité MS09-013 de Microsoft pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS09-013 du 14 avril 2009 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS09-013.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS09-013.msp>
- Référence CVE CVE-2009-0086 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0086>
- Référence CVE CVE-2009-0089 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0089>
- Référence CVE CVE-2009-0550 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0550>

Gestion détaillée du document

15 avril 2009 version initiale.