Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 15 avril 2009
N° CERTA-2008-ALE-012-001

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité dans Microsoft Windows

Gestion du document

Référence	CERTA-2008-ALE-012-001
Titre	Vulnérabilité dans Microsoft Windows
Date de la première version	10 octobre 2008
Date de la dernière version	15 avril 2009
Source(s)	Bloc-note de Microsoft Security Response Center du 09 octobre 2008
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

– Elévation de privilèges.

2 Systèmes affectés

– Microsoft Windows XP Service Pack 2 et Service Pack 3 ;
– Microsoft Windows Vista et Service Pack 1 ;
– Microsoft Windows Vista x64 Edition et Service Pack 1 ;
– Microsoft Windows Server 2003 Service Pack 1 et Service Pack 2 ;
– Microsoft Windows Server 2003 x64 Edition et x64 Edition Service Pack 2 ;
– Microsoft Windows Server 2003 Service Pack 1 et Service Pack 2 pour système Itanium ;
– Microsoft Windows Server 2008 32-bit, x64 et système Itanium.

3 Résumé

Une vulnérabilité dans Microsoft Windows permet à un utilisateur malintentionné d'élever ses privilèges à ceux de `LocalSystem`.

4 Description

Une vulnérabilité dans Microsoft Windows permet à un utilisateur malveillant, authentifié sur le système avec le compte `NetworkService` ou `LocalService`, d'élever ses privilèges au moyen d'un code exécutable malveillant.

Le service `Internet Information Services` (`IIS`) ou encore `SQL Server` permettent à un utilisateur d'accéder au système avec les comptes lui permettant d'exploiter la vulnérabilité décrite. Cependant, Microsoft annonce que tout service bénéficiant des privilèges `SeImpersonatePrivilege` peut être vulnérable et être utilisé par un individu malintentionné pour élever ses privilèges sur le système.

Cette vulnérabilité implique que l'utilisateur malveillant puisse télécharger et exécuter sur le serveur vulnérable un fichier exécutable malveillant.

Le savoir-faire nécessaire pour exploiter cette vulnérabilité est disponible sur l'Internet et peut être modifié par un utilisateur malveillant afin d'élever ses privilèges au travers d'autres services qu'`Internet Information Services` ou `SQL Server`.

5 Contournement provisoire

Microsoft propose trois contournements provisoires pour le service `Internet Information Service` version 6.0 et 7.0 à l'adresse suivante :
http://www.microsoft.com/technet/security/advisory/951306.mspx

Le CERTA recommande les actions suivantes :

- interdire l'exécution de programme tiers par les services vulnérables accessibles depuis une zone non-sûre ;
- interdire le téléchargement de fichiers distants sur le serveur ;
- vérifier le contenu des fichiers téléchargés sur le serveur ;
- autoriser l'accès au serveur uniquement aux utilisateurs de confiance.

6 Solution

Se référer au bulletin de sécurité MS09-012 de Microsoft pour l'obtention des correctifs (cf. section Documentation). Ce dernier est présenté dans l'avis CERTA-2009-AVI-142 du 15 avril 2009.

7 Documentation

- Bloc-note de Microsoft Security Response Center du 09 octobre 2008 :
  http://blogs.technet.com/msrc/archive/2008/10/09/update-1-microsoft-security-advisory-951306.aspx
- Bulletin de sécurité Microsoft #951306 du 17 avril 2008 :
  http://www.microsoft.com/technet/security/advisory/951306.mspx
- Référence CVE CVE-2008-1436 :
  http://www.cve.mitre.org/cgi-bin/cvename=CVE-2008-1436
- Avis du CERTA CERTA-2009-AVI-142 du 15 avril 2009 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2009-AVI-142/
- Bulletin de sécurité Microsoft MS09-012 du 14 avril 2009 :
  http://www.microsoft.com/france/technet/security/Bulletin/MS09-012.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS09-012.mspx

Gestion détaillée du document

10 octobre 2008 version initiale.

15 avril 2009 ajout des références au bulletin de sécurité Microsoft MS09-012.