Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 juillet 2011
N° CERTA-2011-AVI-390

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans CSRSS de Microsoft Windows

Gestion du document

Référence	CERTA-2011-AVI-390
Titre	Multiples vulnérabilités dans CSRSS de Microsoft Windows
Date de la première version	13 juillet 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft du 12 juillet 2011
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

Élévation de privilèges.

2 Systèmes affectés

- Windows XP Service Pack 3 ;
- Windows XP Professional x64 Edition Service Pack 2 ;
- Windows Server 2003 Service Pack 3 ;
- Windows Server 2003 x64 Edition Service Pack 2 ;
- Windows Server 2003 avec Service Pack 2 pour Itanium ;
- Windows Vista Service Pack 1 et Windows Vista Service Pack 2 ;
- Windows Vista x64 Edition Service Pack 1 et Service Pack 2 ;
- Windows Server 2008 32 bits et Windows Server 2008 32 bits Service Pack 2 ;
- Windows Server 2008 64 bits et Windows Server 2008 64 bits Service Pack 2 ;
- Windows Server 2008 pour Itanium et Windows Server 2008 pour Itanium Service Pack 2 ;
- Windows Server 2008 32 bits et Windows Server 2008 32 bits Service Pack 2 ;
- Windows 7 32 bits et Windows 7 32 bits Service Pack 1 ;
- Windows 7 64 bits et Windows 7 64 bits Service Pack 1 ;

- Windows Server 2008 R2 32 bits et Windows Server 2008 R2 32 bits Service Pack 2 ;
- Windows Server 2008 R2 64 bits et Windows Server 2008 R2 64 bits Service Pack 2 ;
- Windows Server 2008 R2 pour Itanium et Windows Server 2008 R2 pour Itanium Service Pack 2.

3 Résumé

Des vulnérabilités permettant une élévation de privilèges ont été découvertes dans *Microsoft Windows*.

4 Description

Des vulnérabilités existent dans le processus `CSRSS` en raison de défauts d'allocation mémoire permettant l'exécution de code arbitraire avec le compte `LocalSystem`.

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 MS11-056 du 12 juillet 2011 :
  http://www.microsoft.com/france/technet/security/Bulletin/MS11-056.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS11-056.mspx
- Référence CVE CVE-2011-1281 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1281
- Référence CVE CVE-2011-1282 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1282
- Référence CVE CVE-2011-1283 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1283
- Référence CVE CVE-2011-1284 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1284
- Référence CVE CVE-2011-1870 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1870

Gestion détaillée du document

13 juillet 2011 version initiale.