Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 11 janvier 2012
N° CERTA-2012-AVI-012

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans les protocoles SSL/TLS dans Microsoft Windows

Gestion du document

Référence	CERTA-2012-AVI-012
Titre	Vulnérabilité dans les protocoles SSL/TLS dans Microsoft Windows
Date de la première version	11 janvier 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS12-006 du 10 janvier 2012
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

Atteinte à la confidentialité des données.

2 Systèmes affectés

- Windows XP Service Pack 3 ;
- Windows XP Professional x64 Edition Service Pack 2 ;
- Windows Server 2003 Service Pack 2 ;
- Windows Server 2003 x64 Edition Service Pack 2 ;
- Windows Server 2003 with SP2 for Itanium-based Systems ;
- Windows Vista Service Pack 2 ;
- Windows Vista x64 Edition Service Pack 2 ;
- Windows Server 2008 for 32-bit Systems Service Pack 2 ;
- Windows Server 2008 for x64-based Systems Service Pack 2 ;
- Windows Server 2008 for Itanium-based Systems Service Pack 2 ;
- Windows 7 for 32-bit Systems and Windows 7 for 32-bit Systems Service Pack 1 ;
- Windows 7 for x64-based Systems and Windows 7 for x64-based Systems Service Pack 1 ;

– Windows Server 2008 R2 for x64-based Systems and Windows Server 2008 R2 for x64-based Systems Service Pack 1 ;
– Windows Server 2008 R2 for Itanium-based Systems and Windows Server 2008 R2 for Itanium-based Systems Service Pack 1.

3 Résumé

Une vulnérabilité des protocoles SSL et TLS implémentés dans les logiciels Microsoft Windows peut porter atteinte à la confidentialité des données.

4 Description

Une vulnérabilité dans les protocoles SSL 3.0 et TLS 1.0 permet à un attaquant de déchiffrer les informations acheminées. Une solution de contournement avait été proposée par Microsoft en septembre 2011 (CERTA-2011-AVI-541) ; un correctif est maintenant disponible.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

– Document du CERTA CERTA-2011-AVI-541 du 29 septembre 2011 :
http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-541/index.html
– Bulletin de sécurité Microsoft MS12-006 du 10 janvier 2012 :
http://technet.microsoft.com/fr-fr/security/bulletin/MS12-006
http://technet.microsoft.com/en-us/security/bulletin/MS12-006
– Référence CVE CVE-2011-3389 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3389

Gestion détaillée du document

11 janvier 2012 version initiale.