

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité dans le sous-système MS-DOS de Microsoft 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-2010-ALE-002>

Gestion du document

Référence	CERTA-2010-ALE-002-002
Titre	Vulnérabilité dans le sous-système MS-DOS de Microsoft Windows
Date de la première version	21 janvier 2010
Date de la dernière version	10 février 2010
Source(s)	
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

Remarque : les versions 64-bit des systèmes d'exploitations de Microsoft ne sont pas affectés par cette vulnérabilité.

- Microsoft Windows 2000 Service Pack 4 ;
- Microsoft XP Service Pack 2 et Windows XP Service Pack 3 ;
- Microsoft Server 2003 Service Pack 2 ;
- Windows Vista, Windows Vista Service Pack 1 et Windows Vista Service Pack 2 ;
- Microsoft Server 2008 ;
- Windows 7.

3 Résumé

Une vulnérabilité dans le sous-système MS-DOS de Microsoft Windows peut être exploitée par un utilisateur local malintentionné afin d'élever ses privilèges.

4 Description

Une vulnérabilité dans le sous-système MS-DOS (`ntvdm.exe`) et affectant potentiellement toutes les versions 32 bits de Microsoft Windows, permet à un utilisateur local d'élever ses privilèges au moyen d'un exécutable spécialement construit.

Le savoir-faire nécessaire pour exploiter cette vulnérabilité est d'ores et déjà disponible sur l'Internet.

5 Contournement provisoire

Le CERTA recommande de désactiver l'accès au sous-système MS-DOS en modifiant les stratégies de groupes.

L'application de ce contournement provisoire peut avoir des effets de bords indésirables. En effet, certaines applications présentes nativement sur un système Microsoft Windows fonctionnent au moyen de l'accès au sous-système MS-DOS. Pour ne citer qu'un exemple, l'exécutable `COMMAND.COM` ne pourra donc plus fonctionner suite à l'application de ce contournement provisoire. Naturellement, tous les scripts faisant appel à des programmes nécessitant l'accès au sous-système MS-DOS ne seront plus opérationnels.

La désactivation du sous-système MS-DOS sous Microsoft Windows peut s'effectuer par les étapes suivantes :

- dans l'outil de configuration des stratégies de groupe, `gpedit.msc` ;
- sélectionner Modèles d'administration puis Composants Windows et enfin Compatibilité des applications ;
- choisir l'élément Empêcher l'accès aux applications 16-bit ;
- cocher l'option Activer dans les propriétés de l'élément.

Ce contournement peut également être appliqué par la modification ou la création de valeurs dans la base de registre du système :

- avec l'éditeur de la base de registre (`regedit.exe`) ;
- sélectionner la clé suivante :
`\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows ;`
- créer la clé `AppCompat` si celle-ci n'existe pas ;
- sélectionner cette nouvelle clé et créer une valeur `VDMDisallowed` avec le type `DWORD` ;
- mettre à 1 la donnée de la valeur précédente ;
ou encore :
- sélectionner la clé :
`\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WOW ;`
- si la valeur `DisallowedPolicyDefault` n'existe pas, la créer avec le type `DWORD` ;
- modifier la donnée de la valeur `DisallowedPolicyDefault` en la mettant à 1.

Microsoft a publié un guide pour désactiver l'accès au sous-système MS-DOS (cf. section Documentation).

6 Solution

Le bulletin de sécurité MS010-015 de Microsoft corrige le problème.

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

7 Documentation

- Bulletin de sécurité Microsoft MS10-015 du 09 février 2010 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS10-015.aspx>
<http://www.microsoft.com/technet/security/Bulletin/MS10-015.aspx>
- Bulletin de sécurité Microsoft #979682 du 21 janvier 2010 :
<http://www.microsoft.com/technet/security/advisory/979682.aspx>
- Guide de Microsoft : « *Disabling the MSDOS and WOWEXEC Subsystems on Terminal Server* » :
<http://support.microsoft.com/kb/220159/>

- Avis de sécurité du CERTA CERTA-2010-AVI-073 du 10 février 2010 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-073/index.html>
- Référence CVE CVE-2010-0232 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0232>

Gestion détaillée du document

21 janvier 2010 version initiale ;

21 janvier 2010 modification de la section « Contournement provisoire » ;

10 février 2010 ajout de la solution, ajout des liens vers le bulletin MS10-015 et vers CERTA-2010-AVI-073.