

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Exploitation par un code malveillant d'une vulnérabilité Microsoft Windows non corrigée

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-009>

Gestion du document

Référence	CERTA-2010-ALE-009-003
Titre	Exploitation par un code malveillant d'une vulnérabilité Microsoft Windows non corrigée
Date de la première version	16 juillet 2010
Date de la dernière version	03 août 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

Exécution de code arbitraire à distance.

2 Systèmes affectés

Microsoft Windows toutes versions.

3 Résumé

Un code malveillant exploitant une vulnérabilité dans Microsoft Windows permet à une personne distante malintentionnée d'exécuter du code arbitraire.

4 Description

Un code malveillant, généralement connu sous le nom de *Stuxnet* ou *CplLnk*, exploite activement une vulnérabilité de Microsoft Windows. Cette vulnérabilité réside dans la gestion des fichiers de raccourcis *.lnk* et permet l'exécution à distance de code arbitraire avec les droits de l'utilisateur connecté sur la machine.

Le code malveillant utilise les périphériques de stockage *USB* pour se propager.

5 Contournement provisoire

Microsoft a publié un contournement permettant de limiter l'exploitation de la vulnérabilité *.lnk*, voir l'alerte CERTA-2010-ALE-010.

En attendant la publication d'un correctif, le CERTA recommande les bonnes pratiques suivantes :

- se connecter avec un compte utilisateur aux droits limités ;
- maintenir à jour la solution antivirus ;
- porter une attention toute particulière à la présence inattendue de fichiers *.lnk*.

6 Moyens de détection

Une fois installé et à la rédaction de ce document, le code malveillant effectue les opérations suivantes :

- il crée les fichiers ci-dessous :
 - %SYSTEM%\system32\drivers\mrxccls.sys ;
 - %SYSTEM%\system32\drivers\mrxcnet.sys ;
 - C:\Windows\inf\mdmcpq3.pnf ;
 - C:\Windows\inf\mdmeric3.pnf ;
 - C:\Windows\inf\oem6c.pnf ;
 - C:\Windows\inf\oem7a.pnf.
- il crée également les clés de registre suivantes :
 - HKLM\SYSTEM\CurrentControlSet\Services\MRxCls ;
 - HKLM\SYSTEM\CurrentControlSet\Services\MRxNet.

De plus, il tente des connexions vers les domaines ci-dessous :

- www.mypremierfutbol.com ;
- www.todaysfutbol.com.

7 Solution

Se référer au bulletin de sécurité Microsoft pour l'obtention du correctif de la vulnérabilité (cf. section Documentation).

8 Documentation

- Bulletin de sécurité Microsoft MS10-046 du 03 août 2010 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS10-046.aspx>
<http://www.microsoft.com/technet/security/Bulletin/MS10-046.aspx>
- Avis CERTA-2010-AVI-353 du 3 août 2010 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-353>
- Alerte CERTA-2010-ALE-010 du 19 juillet 2010 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2010-ALE-010>
- Description du code malveillant *Stuxnet* par le Microsoft Malware Protection Center :
<http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=TrojanDropper%3aWin32%2fStuxnet.A>
- Description du code malveillant *CplLnk* par le Microsoft Malware Protection Center :
<http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Exploit%3aWin32%2fCplLnk.A>

Gestion détaillée du document

16 juillet 2010 version initiale ;

16 juillet 2010 correction dans les liens Microsoft ;

19 juillet 2010 modification des sections Contournement et Documentation ;

03 août 2010 ajout de la section Solution et ajout de la référence au bulletin de sécurité Microsoft dans la section Documentation.