Le **CERT** dédié à la communauté **Industrie, Services et Tertiaire** française

Ver "Conficker" sur les systèmes Microsoft Windows

Référence : CERT-IST/AV-2008.504
Version : 1.3
Date de la version : 02 Février 2009

Classification de la vulnérabilité

Risque : Très élevé
Conséquence : Prise de contrôle du système
Niveau de connaissance de l'attaquant : Novice
Moyen nécessaire à l'attaquant : A distance sans compte via un service standard

Information sur le(s) système(s) impacté(s)

Plate(s)-forme(s) impactée(s) :

- Windows 2000 SP4
- Windows XP SP2 et SP3
- Windows XP Professional x64 Edition et Windows XP Professional x64 Edition SP2
- Windows Server 2003 SP1 et Windows Server 2003 SP2
- Windows Server 2003 SP1 (Itanium) et Windows Server 2003 SP2 (Itanium)
- Windows Server 2003 x64 Edition et Windows Server 2003 x64 Edition SP2
- Windows Vista et Windows Vista SP1
- Windows Vista X64 Edition et Windows Vista X64 Edition SP1
- Windows Server 2008 pour les systèmes 32-bit, 64-bit et Itanium

Logiciel(s) impacté(s) :

- NA

Remarques :

- Les systèmes 'patchés' avec les correctifs du bulletin MS08-067 ne peuvent être infectés par ce ver.

Liste exhaustive des produits du catalogue Cert-IST impactés :

Description

Nature du problème :

"Conficker" est un ver informatique qui se propage via les réseaux locaux des machines infectées, en exploitant la vulnérabilité RPC du service "Serveur" **(MS08-067)**des systèmes Microsoft Windows, décrite dans l'avis**CERT-IST/AV-2008.460.**

"Conficker" tente d'ouvrir une porte dérobée sur les systèmes infectés.

Nota : "Conficker" est aussi connu sous les noms**"Confick", "Downadup"**ou**"Downad".**

Analyse détaillée :

En plus du comportement général donné précédemment, on notera les points suivants :

- "Conficker" lance un serveur HTTP sur un port aléatoire sur les systèmes infectés afin d'héberger une copie du ver.
- "Conficker" sonde le réseau (scan) pour détecter des machines vulnérables à la faille**MS08-067.**Lorsqu'il en trouve, la machine distante se connecte sur le serveur HTTP et télécharge une copie du ver.
- Sous Windows 2000, "Conficker" injecte une copie de son code malicieux dans le processus "services.exe".
- Sous les autres systèmes, "Conficker" crée un service ayant pour nom "netsvcs".
- "Conficker" tente d'appeler une API afin de réinitialiser le point de restauration du système infecté, ce qui peut faire échouer les tentatives de restauration ultérieures.

Solution

Solution à l'infection du ver "Conficker"

Mettre à jour votre outil d'anti-virus afin de prendre en compte le ver décrit :

- Utiliser le mécanisme de mise à jour automatique de votre anti-virus.
- Ou utiliser les indications données ci-dessous afin de mettre à jour manuellement votre anti-virus.
- Mises à jour de l'éditeur Computer Associates
  - http://www3.ca.com/support/vicdownload/
- Mise à jour de l'éditeur F-Secure - date de la mise à jour : 26/11/2008 ou utiliser les mises à jour suivantes
  - ftp://ftp.f-secure.com/anti-virus/updates/fsupdate.exe
  - http://f-secure.com/download-purchase/latest.zip
- Mise à jour de l'éditeur NAI - fichier DAT 5444 du 24/11/2008 ou utiliser les mises à jour suivantes
  - http://download.nai.com/products/mcafee-avert/daily_dats/DAILYDAT.ZIP
  - http://download.nai.com/products/mcafee-avert/daily_dats/SDATDAILY.EXE
- Mise à jour de l'éditeur Sophos - fichier fournissant la signature du ver
  - http://www.sophos.com/downloads/ide/436_ides.zip
- Mise à jour de l'éditeur Symantec - outils "Intelligent Updater" (lien ci-dessous) et "LiveUpdate" mis à jour du 26/11/2008

    - http://securityresponse.symantec.com/avcenter/defs.download.html
- Mise à jour de l'éditeur TrendMicro - fichier de signature 5.679.00 ou supérieur
    - http://www.trendmicro.com/ftp/products/pattern/lpt679.zip
    - http://www.trendmicro.com/ftp/products/pattern/lpt679.tar

Note(s) CVSS

- Cert-IST - CERT-IST/AV-2008.504
    - Base score : 10.0 - AV:A/AC:L/Au:N/C:C/I:C/A:C
    - Score temporaire : 7.4 - AV:A/AC:L/Au:N/C:C/I:C/A:C/E:U/RL:OF/RC:C

Identifiant(s) du problème

- CVE: CVE-2008-4250

Documentation additionnelle

- Document de F-Secure concernant le ver "Conficker"
    - http://www.f-secure.com/v-descs/worm_w32_downadup_a.shtml
- Document de NAI concernant le ver "Conficker"
    - http://vil.nai.com/vil/content/v_153464.htm
- Documents de Sophos concernant le ver "Conficker"
    - http://www.sophos.com/security/analyses/viruses-and-spyware/w32conficka.html http://www.sophos.com/security/analyses/viruses-and-spyware/malconfickera.html
- Document de Symantec concernant le ver "Conficker"
    - http://www.symantec.com/business/security_response/writeup.jsp?docid=2008-112203-2408-99
- Document de TrendMicro concernant le ver "Conficker"
    - http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_DOWNAD.A&VSect=P
- Document de Computer Associates concernant le ver "Conficker"
    - http://www.ca.com/us/securityadvisor/virusinfo/virus.aspx?id=75911
- Document de Panda concernant le ver "Conficker"
    - http://www.pandasecurity.com/enterprise/security-info/about-malware/encyclopedia/overview.aspx?IdVirus=202881
- Alerte de Microsoft concernant la variante Conficker.B (KB962007)
    - http://support.microsoft.com/kb/962007

Version	Commentaire	Date
1.0	Création de l'avis	27/11/2008
1.1	Précisions concernant les sites contactés par le ver	28/11/2008
1.2	Second document de Sophos concernant le ver "Conficker"	05/01/2009
1.3	Alerte de Microsoft concernant la variante Conficker.b	02/02/2009