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

Détail de l'alerte

Propagation du ver "Conficker" (vulnérabilité MS08-067)

Référence : CERT-IST/AL-2008.002
Version : 1.0
Date de la version : 27 Novembre 2008

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 for 32-bit, 64-bit et Itanium systems

Logiciel(s) impacté(s) :

- NA

Liste exhaustive des produits du catalogue Cert-IST impactés :

Description

Nature du problème :

Nous émettons cette alerte car nous avons eu confirmation de rapports d'infection par le ver "Conficker" au sein de notre communauté IST. Le ver "Conficker" est décrit dans l'avis**CERT-IST/AV-2008.504.**Ce ver se propage en exploitant la vulnérabilité RPC du service "Serveur" (MS08-067) des systèmes Microsoft Windows et permet d'ouvrir une porte dérobée sur les systèmes infectés.

Il semblerait que certaines variantes de "Conficker" ne soient pas correctement détectées par les anti-virus (même à jour). Nous vous recommandons donc de bloquer les URL utilisées par le ver (voir solution 02).

Les systèmes ayant appliqué les correctifs indiqués dans le bulletin MS08-067 ne sont pas impactés.

Solution

01 - Appliquer les solutions décrites dans l'avis CERT-IST/AV-2008.460

L'avis CERT-IST/AV-2008.460 indique les correctifs Microsoft à appliquer pour corriger la vulnérabilité MS08-067 de Windows.
Il donne aussi les mesures palliatives ainsi que les moyens de détecter l'exploitation de cette vulnérabilité.

02 - Bloquer les sites web contactés par "Conficker"

Certains éditeurs anti-virus semblent ne pas détecter complètement le ver "Conficker" (ou ses variantes). Une solution temporaire est de filtrer les sites suivants au niveau des passerelles Internet :

[http://]trafficconverter.biz/4vir/antispyware/loada[retiré]

[http://]www.maxmind.com/download/geoip/database/GeoIP.[retiré]

"Conficker" tente également de contacter les sites suivants afin de récupérer l'adresse IP du système infecté :
[http://]www.getmyip.org
[http://]/getmyip.co.uk
[http://]checkip.dyndns.org

Le ver tente également de contacter les sites suivants afin d'obtenir la date courante :
[http://]www.w3.org
[http://]www.ask.com
[http://]www.msn.com
[http://]www.yahoo.com
[http://]www.google.com
[http://]www.baidu.com

Note(s) CVSS

- Cert-IST - CERT-IST/AL-2008.002
  - Base score : -
  - Score temporaire : -

Identifiant(s) du problème

- CVE: CVE-2008-4250

Documentation additionnelle

- Blog de Microsoft concernant les tentatives d'exploitation MS08-067
  - http://blogs.technet.com/mmpc/archive/2008/11/25/more-ms08-067-exploits.aspx
- Archive du SANS du 26 novembre 2008
  - http://isc.sans.org/diary.html?storyid=5401
- Blog de Trend Micro concernant les tentatives d'exploitation MS08-067
  - http://blog.trendmicro.com/ms08-067-vulnerability-botnets-reloaded/

Version	Commentaire	Date
1.0	Création de l'alerte	27/11/2008